SEGURIDAD ELECTRÓNICA

SISTEMAS

Contenidos

- Introducción a los sistemas electrónicos de Seguridad
- Detección de intrusión
- Videovigilancia
- Control de accesos
- Detección y extinción de incendios
- Sistemas integrados

Agenda de la Jornada

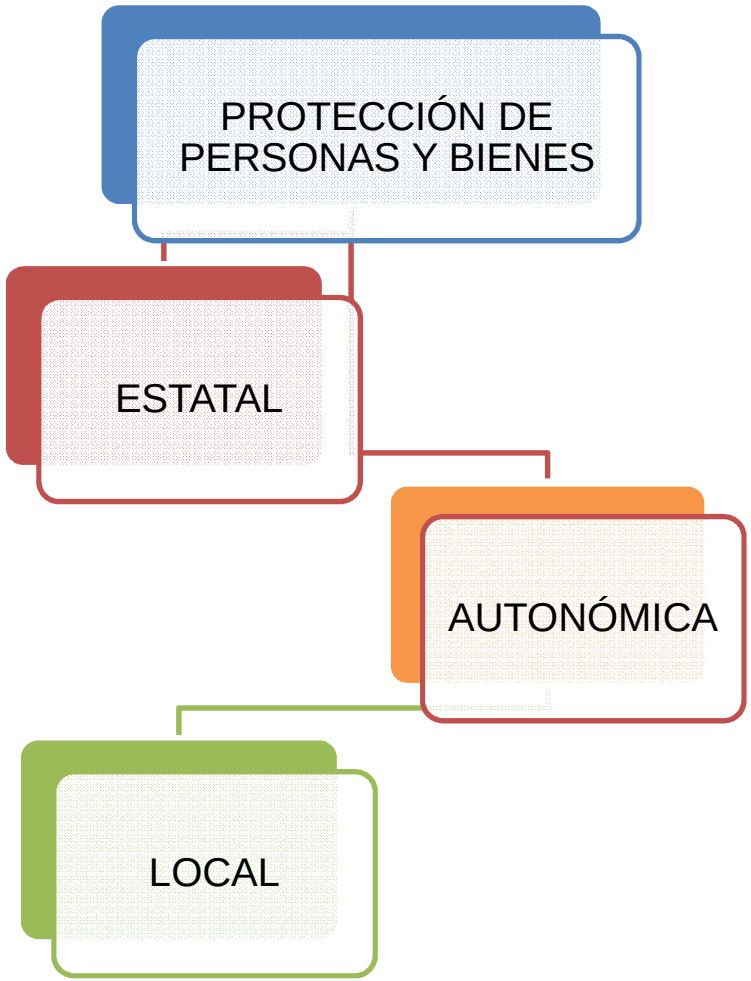
09:30	Recepción asistentes
09:45 a 11:15	Sistemas de seguridad
11:15 a 11:45	Pausa
11:45 a 12:15	Detección de intrusión
12:15 a 12:45	Videovigilancia y legislación
12:45 a 13:00	Control de accesos e integración
13:00 a 13:30	Demostración extinción
13:30	Preguntas

© Casmar Electrónica, SA - Confidencial

Video corporativo CASMAR

Sistemas de seguridad
Contextualización

Contexto Legislativo



- **Ley 1/92, de 21 de febrero, de Seguridad Ciudadana**
- **Ley 23/1992, de 30 de Julio, de Seguridad Privada**
- **Real Decreto 2364/1994, de 9 de diciembre; Reglamento de Seguridad Privada**
- **Órdenes Ministeriales**
- **Reglamentaciones autonómicas o locales:**
  - IRP/198/2010 GENCAT
  - Norma técnica protección de edificios públicos de uso administrativo (Junta Andalucía)
  - Ordenanzas municipales

Sistemas de seguridad

- **A efectos de Seguridad Privada:**

  - Son los conjuntos de dispositivos electrónicos y aparatos cuya activación sea susceptible de producir intervención policial, independientemente de su conexión a CRA o Centro de Control

  - Forma parte de las instalaciones todo aquello que las complemente automática, material o procedimentalmente incluyendo CCAA y CCTV

Homologación del material de instalaciones

- **Aprobados** conforme a las normas europeas
  - ✓ UNE-EN 50130 / 50131 / 50132 / 50133 / 50136 / 50398
- La modificación o aprobación de cualquier norma UNE sobre esta materia será suficiente para su aplicación **inmediata** a las nuevas instalaciones

Relación de Normas UNE-EN (relativas a sistemas)

Normas EN	Aspectos que cubre
50130-4 y 5	Sistemas de alarma. Compatibilidad electromagnética. Métodos ensayo ambiental
50131	Sistemas de alarma
50132	Sistemas vigilancia CCTV para uso en aplicaciones de seguridad
50133	Sistemas de control de accesos para uso en aplicaciones de seguridad
50134	Sistemas de alarma social
50136	Sistemas y equipos de transmisión de alarmas
50398	Sistemas de alarma combinados o integrados

Grados de Seguridad

Grado Seguridad	Descripción
1	Bajo riesgo, para sistemas de seguridad dotados de señalización acústica y sin conexión a central de alarmas
2	Riesgo bajo/medio, dedicado a viviendas y pequeños establecimientos en general, conectados a una central de alarmas o centro de control
3	Riesgo medio/alto, para establecimientos obligados a disponer de medidas de seguridad, así como instalaciones comerciales que por su actividad sea aconsejable
4	Riesgo alto, destinado a infraestructuras críticas, instalaciones militares, depósitos de efectivo, valores o metales preciosos

Clase Ambiental

Clase Ambiental	Descripción
I	Interior. Esta clase cubre los elementos que funcionarán en ambientes en interior donde la temperatura se mantiene bastante uniforme. +5 a +40ºC
II	Interior General. Esta clase cubre los detectores, teclados, centrales de seguridad y otros dispositivos. Especifica que dichos elementos deberán funcionar en un entorno en el que puede haber variaciones de temperatura importantes o condensaciones en ventanas y áreas de almacenamiento -10 a +40ºC
III	Exterior a cubierto o interior en condiciones extremas. Especifica que dichos elementos no estarán totalmente expuestos en exteriores, o estarán en interiores en condiciones extremas. -25 a +50ºC
IV	Exterior General. Esta clase cubre las sirenas y otros elementos instalados en exteriores, los cuales estarán totalmente expuestos a las inclemencias ambientales. -25 a +60ºC

Normas Europeas EN50131

Normas EN 50131	Aspectos que cubre
50131-1	Requisitos generales sistemas de alarma contra intrusión y atraco
50131-2	Requisitos sobre dispositivos de detección
50131-3	Requisitos sobre central y teclados
50131-4	Requisitos sobre los dispositivos de advertencia, sirenas, etc.
50131-5	Requisitos sobre interconexiones, cableado, enlaces inalámbricos, etc.
50131-6	Requisitos sobre fuentes de alimentación
50131-7	Guía de aplicación
50131-8	Requisitos dispositivos de niebla de seguridad

Elementos obligados a estar certificados

Elemento	Descripción	Normas	
	Central intrusión y teclados	UNE-EN 50131-**1**/A1:2010 UNE-EN 50131-**3**:2010	UNE-EN 50131-**1**:2008
	Elementos Vía Radio	UNE-EN 50131-**5-3**:2005/A1:2008	
	Volumétricos	UNE-EN 50131-**2-2**:2008 (IR) UNE-EN 50131-**2-3**:2009 (MW) UNE-EN 50131-**2-4**:2008 (IR+MW) UNE-EN 50131-**2-5**:2009 (IR+US)	
	Contactos magnéticos	UNE-EN 50131-**2-6**:2009	
	Sirenas	UNE-EN 50131-**4**:2010	
	Fuentes de alimentación	UNE-EN 50131-**6**:2008	
	Generadores de niebla	UNE-EN 50131-**8**:2009	

Otros elementos

Elemento	Descripción	Normas
	Barreras de infrarrojos activos	
	Volumétricos de exterior	
	Barreras de microondas	
	Cable sensor	
	Pulsad es a ra	

NO SE CERTIFICAN

Períodos de Adaptación

- **Cuando un sistema necesite utilizar componentes que en el momento de su instalación no estén disponibles se permitirá su conexión hasta:**

  - **La posible aparición de la norma que lo regule**
  - **Disponibilidad en el mercado**
  - **En ese momento, se deberá sustituir**
    - ✓ **Máximo en el periodo de adecuación (10 ó 2 años)**

Certificación de producto

Objetivo

- Homogenizar las diferentes normativas existentes en los países miembros de la Unión Europea para que las condiciones técnicas y de seguridad sean equivalentes a las exigidas en cada uno de ellos

Finalidad perseguida con su adopción

- Mejorar la calidad e integridad de los sistemas
- Mejorar la profesionalidad del sector de la seguridad.

Organismos

Comité Europeo de Normalización Electrotécnica es el organismo europeo de normalización para la electrónica. Las normas elaboradas por CENELEC tienen que ser adoptadas, sin ninguna modificación, por los miembros nacionales de estandarización europeos.

CENELEC genera y aprueba los siguientes tipos de documentos:

- **EN - European Standard**
- **HD - Harmonization Document**
- **TS - Technical Specification**
- **TR - Technical Report**
- **G - Guides**
- **CWA - CENELEC Workshop Agreement**

Organismos

AENOR

AENOR es una entidad dedicada al desarrollo de la normalización y la certificación en todos los sectores industriales y de servicios.
Es la única entidad reconocida en España para desarrollar las tareas de normalización y certificación y para representar al país ante los organismos internacionales, europeos y regionales: ISO, IEC, CEN, CENELEC, ETSI, COPANT

Normas UNE (Una Norma Española)
Son el nombre que reciben las normas elaboradas por AENOR. Cuando un estándar EN se incorpora a España, éste va precedido por la siglas UNE – EN .....

© Casmar Electrónica, SA - Confidencial

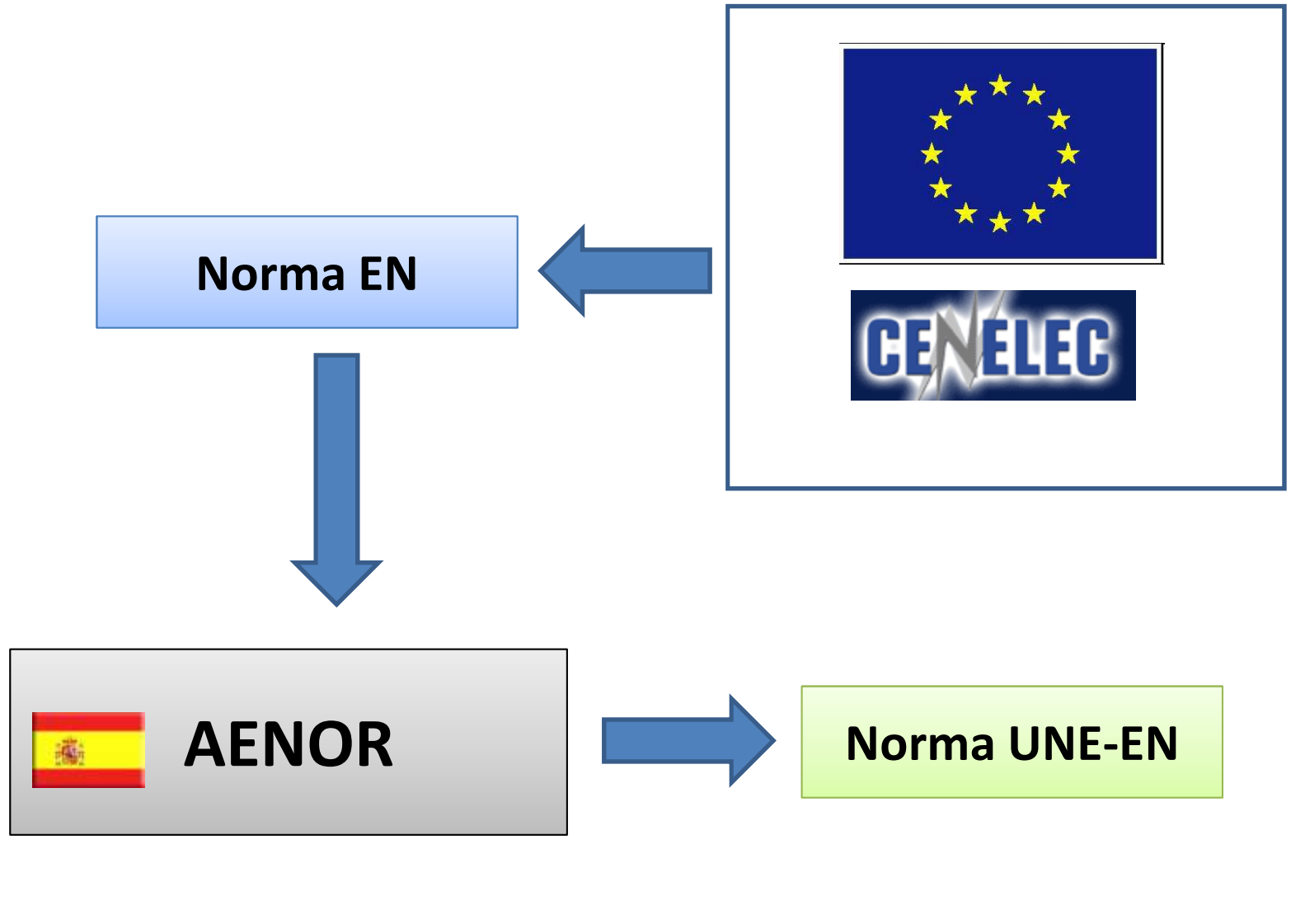
Organismos

ENAC
Entidad Nacional de Acreditación

ENAC tiene como misión generar confianza en el mercado y en la sociedad en general en relación con la competencia técnica de los evaluadores de la conformidad acreditados.

Es la única entidad, en España, que puede acreditar los laboratorios

Procedimiento de Normalización



Procedimiento de certificación

Creación de Normas EN	
CENELEC	Comité Técnico TC 79
Diseño y Fabricación	
Fabricante	Conforme normas EN
Evaluación Conformidad	
Laboratorio Externo	ISO-17025
Certificación	
Organismo Acreditado	EN-45011

© Casmar Electrónica, SA - Confidencial

Sistemas de certificación ISO

NIVEL	TIPO DE ENSAYO
1	Ensayo de tipo
2	Ensayo de tipo + control en mercado
3	Ensayo de tipo + control en fábrica
4	Ensayo de tipo + control en el mercado control en fábrica
5	Ensayo de tipo + evaluación del sistema de la calidad + control en el mercado+ control en fábrica
6	Evaluación del sistema de la calidad
7	Certificación por lotes
8	Ensayo al 100%

DET NORSKE VERITAS

CERTIFICATE OF CONFORMITY

Certificate No. 70101-2010-PC-NOR-NA, Rev 2
This Certificate consists of 4 pages

This is to certify that the product

Intrusion Alarm Central with Peripheral Equipment

with name type designations

manufactured by

[redacted]

EN 50131 Grade 3 environmental Class II

including relevant underlying normative references has found to comply with the applicable requirements.
Further details are given overleaf

Place and date:		*This Certificate is valid until:*
Høvik, 16.02.2010	NORWEGIAN ACCREDITATION PROD 002	29.01.2015
for DET NORSKE VERITAS CERTIFICATION AS		
Norway		
Marianne Spæren		Steinar Kristensen
Certification Manager (ZNWNO416)		*Technical Reviewer*

Notice: The certificate is subject to terms and conditions overleaf. Any significant changes in design or construction may render this certificate invalid.

If any person suffers loss or damage which is proved to have been caused by any negligent act or omission of Det Norske Veritas, then Det Norske Veritas shall pay compensation to such person for his proved direct loss or damage. However, the compensation shall not exceed an amount equal to ten times the fee charged for the service in question, provided that the maximum compensation shall never exceed USD 300 000. In this provision "Det Norske Veritas" shall mean the Foundation Det Norske Veritas as well as all its subsidiaries, directors, officers, employees, agents and any other acting on behalf of Det Norske Veritas.

Applied Standards/Tests carried out

Applied Standards
EN 50130-4:1995+A1(1998)+A2(2003)
EN 50131-1:2006
EN 50130-5:1998
EN 50131-6:2008 / EN 50131-6:1997* / **
EN 60950:2001
CLC/TS 50131-3:2003

** CLC/TS 50131-3:2003 refers to EN 50136-5:2007. However, ch.4.2.1 in the 97 version has a requirement that a low voltage situation in SD is detected within 10 sec. In practice 20 sec is required to do such a test properly, so in theory it is impossible to fulfill this requirement. This has been corrected in the 2008 version where this requirement is 5 min. The equipment uses 30 sec to detect a low voltage condition. For this reason, reference to the 2008 version is included.*

***Deep discharge protection triggered when the battery voltage fell below 9.5 V. (The EN 50131-6:1997 requires deep discharge protection to be specified by the storage device manufacturer. According to a number of storage device manufacturers the discharge voltage should not be below10.2 V – 10.5 V. The new EN 50131-6:2008 requires deep discharge protection to be specified by the power supply manufacturer, thus the EUT fulfils the requirements according to EN 50131-6:2008. The latest published version of EN 50131-6 is from 2008, however EN 50131-6:1997was used because CLC/TS 50131-3:2003 refers to the 1997 version of EN50131-6.)*

Documents reviewed

Name	Description
Hardware and Firmware clarification	Hardware and Firmware clarification.pdf
Similarity statement Premier Elite SMK and Premier LCD LP EN.doc	20100422123042849.pdf
Authorisation letter 50950 PSU200 PSU200XP P48 P88 P168 EN50130 COM300 COM2400	55-0135 Texecom LETTER OF AUTHORISATION LETTER.pdf
CB Certificate 50950 PSU200 PSU200XP P48	CB0198Z.pdf
Test Report 50130-4 P168 PCOM-LP P2400 PSU2400XP P48XP ProLCD	EN50130-4 A1 A2 60978765EM1.pdf
Test Report 50130-4 Pro40 PCOM-LP PRCD P	3681703.pdf
Test Report 60950 PSU200 PSU200XP P48 P88 P168 Pro40 COM300 COM2400 rev 2.pdf	55-0135 Texecom report SA 2020 CE1
Test Report EN 50130-5, EN 50130-6	Technical Report 2009-3079 rev 3.pdf

telefication bv
The Netherlands
Chamber of Commerce
09076358
www.telefication.com

telefication

Certificate of Type-examination

No: 06229519/AA/00

Telefication declares that the stated alarm equipment complies with the Technical specifications as listed in Annex 2 of this certificate.

Product description:	**Control and Indicating Equipment for Intruder Alarm System**
Trademark:	**See annex 3**
Family name:	**--**
Type designation:	**See annex 3**
Serial No:	**See annex 3**
Software release No:	**See annex 3**
Manufacturer:	[redacted]
Address:	**Newhouse Industrial Estate**
City:	**Motherwell ML1 5SB**
Country:	**United Kingdom**

This certificate is granted to:

Name:	[redacted]
Address:	**Newhouse Industrial Estate**
City:	**Motherwell ML1 5SB**
Country:	**United Kingdom**

This certificate has THREE Annexes.

Zevenaar, 05 December 2006

CAB

M.H. Koop
Manager Certification

PRODUCTS
RvA C 224

laboratory certification approvals

Remarks and observations

The following conditions are applicable:

Equipment Security grade: Grade 2
Equipment Environmental class: Class II
Equipment class: Fixed

According to prEN 50131-1:2004, this equipment can be applied in installed systems up to and including security grade 2.

Alarm Transmission System classification according to EN 50136-1-1:1998+A1:2201:
For C043-36 PSTN interface of main: D2, M2, T2, S0, I0.
According prEN 50131-1:2004, it can be applied in installed systems up to and including ATS 2.

Note that variants identified by customer variant extensions "xx" in the product number Cnnn-xx are in general differences in labeling and installation instructions. They do not affect the results for EMC, safety and telecommunications tests.

Pôle européen de sécurité CNPP–Vernon
Division Electronique de Sécurité
Route de la Chapelle Réanville
CD 64 - BP 2265
F 27950 SAINT MARCEL
Téléphone 33 (0)2 32 53 64 49
Télécopie 33 (0)2 32 53 64 96

CNPP

Expert en prévention et en maîtrise des risques

SYNTHESE DE RAPPORT D'ESSAIS
SYNTHESIS OF TESTS REPORT

SYSTEMES D'ALARME CONTRE L'INTRUSION

INTRUSION ALARM SYSTEMS

DEMANDE PAR *REQUESTED BY*	: [redacted]
NOM COMMERCIAL *TRADE NAME*	: [redacted] *(composition : voir annexe ; see annex)*
TYPE DE PRODUIT *PRODUCT TYPE*	: CENTRALE D'ALARME *CONTROL AND INDICATING EQUIPMENT*
NORMES DE REFERENCE *REFERENCE STANDARDS*	: TS 50131-3 (2003), EN 50131-6 (1997)
CLASSIFICATION	: Grade 3 Environnement Classe II
SELON RAPPORT D'ESSAIS *BASED ON TESTS REPORT*	: **N° AI 08 00 15 du 17 Avril 2008**
CONCLUSION *CONCLUSION*	: **Le produit testé satisfait aux exigences d'essais des normes citées, pour le grade identifié.** : *The product tested fulfils the tests requirements of the quoted standards, for the identified classification.*

Etablie à St Marcel par le **CNPP – Division Electronique de Sécurité**
Established in St-Marcel by CNPP – Division Electronique de Sécurité

Date : 04/03/2010

Cachet et signature du directeur :
Stamp and signature of the manager

Pôle européen de sécurité CNPP-Vernon
Division Electronique de Sécurité
Laboratoire Electronique de Sécurité
Le directeur
L RIN
Signature électronique

Ce rapport d'essai atteste uniquement des caractéristiques de l'échantillon soumis aux essais et ne préjuge pas des caractéristiques de produits similaires. Il ne constitue donc pas une certification de produits au sens de l'article L.115-27 du code de la consommation et de la loi du 3 juin 1994, ni un agrément ou une qualification de quelque nature que ce soit. La reproduction de ce rapport d'essais n'est autorisée, sauf approbation préalable du CNPP, que sous sa forme intégrale.
Le CNPP décline toute responsabilité en cas de reproduction ou publication non conforme. Le CNPP se réserve le droit d'utiliser les enseignements qui résultent du présent rapport d'essais pour les inclure dans des travaux de synthèse ou d'intérêt général. Les travaux envisagés pouvant être publiés par ses soins.

This test report gives evidence only of characteristics of the sample subjected to the tests and does not prejudge characteristics of similar products. It does not thus constitute a certification of products in the sense of the article L.115-27 of the code of the consumption and the law of June 3rd, 1994, nor an approval or a qualification whatever nature it is. The reproduction of this test report is not authorized, except preliminary approval of CNPP, only under its complete form.
CNPP declines any responsibility in case of reproduction or not corresponding publication. CNPP reserves the right to use the information which result from the present test report to include them in works of synthesis or general interest, the envisaged work which can be published by its care.

[redacted]

Declaration of Conformity

ISSUED BY [redacted]
165 Eileen Way
P.O. Box 9035
Syosset NY 11791
United States of America

MANUFACTURER: [redacted]

DATE OF ISSUE: 6 January 2005

TYPE OF EQUIPMENT: Alarm system control panel

MODEL NUMBERS [redacted]

The products listed above are in conformity with the following standards:

EN 61000-6-3:2001 *Generic Standards - Emission standard for residential, commercial and light-industrial environments*

EN 50130-4:1995 +A1:1998 +A2:2003 *Product family standard: Immunity requirements for components of fire, intruder and social alarm systems*

EN 60950:2000* *Safety of information technology equipment*

* when installed according to relevant electrical codes

in accordance with the provisions of Council Directive(s):

89/336/EEC Electromagnetic compatibility directive

73/23/EEC Low voltage directive

Signed on behalf of at: Syosset NY, U.S.A.

by

Steve Amodeo Vice President, QA

1/7/05
Date

Serial number: DC0020 01/2005

Identificación

Cada componente del sistema debe ser etiquetado con:

a) El fabricante o proveedor
b) El tipo
c) Fecha de fabricación/nº de lote/nº de serie
d) El grado
e) Clase ambiental

© Casmar Electrónica, SA - Confidencial

Identificación

Debe mostrarse la marca CE por ser un producto electrónico y estar dentro del alcance de las Directivas de nuevo enfoque (New approach)

Si el Marcado CE no aparece en un producto, ese producto no cuenta con la autorización para comercializarse libremente en la Unión Europea.

Ejemplo de la realidad del sector

casmar

the coffee break

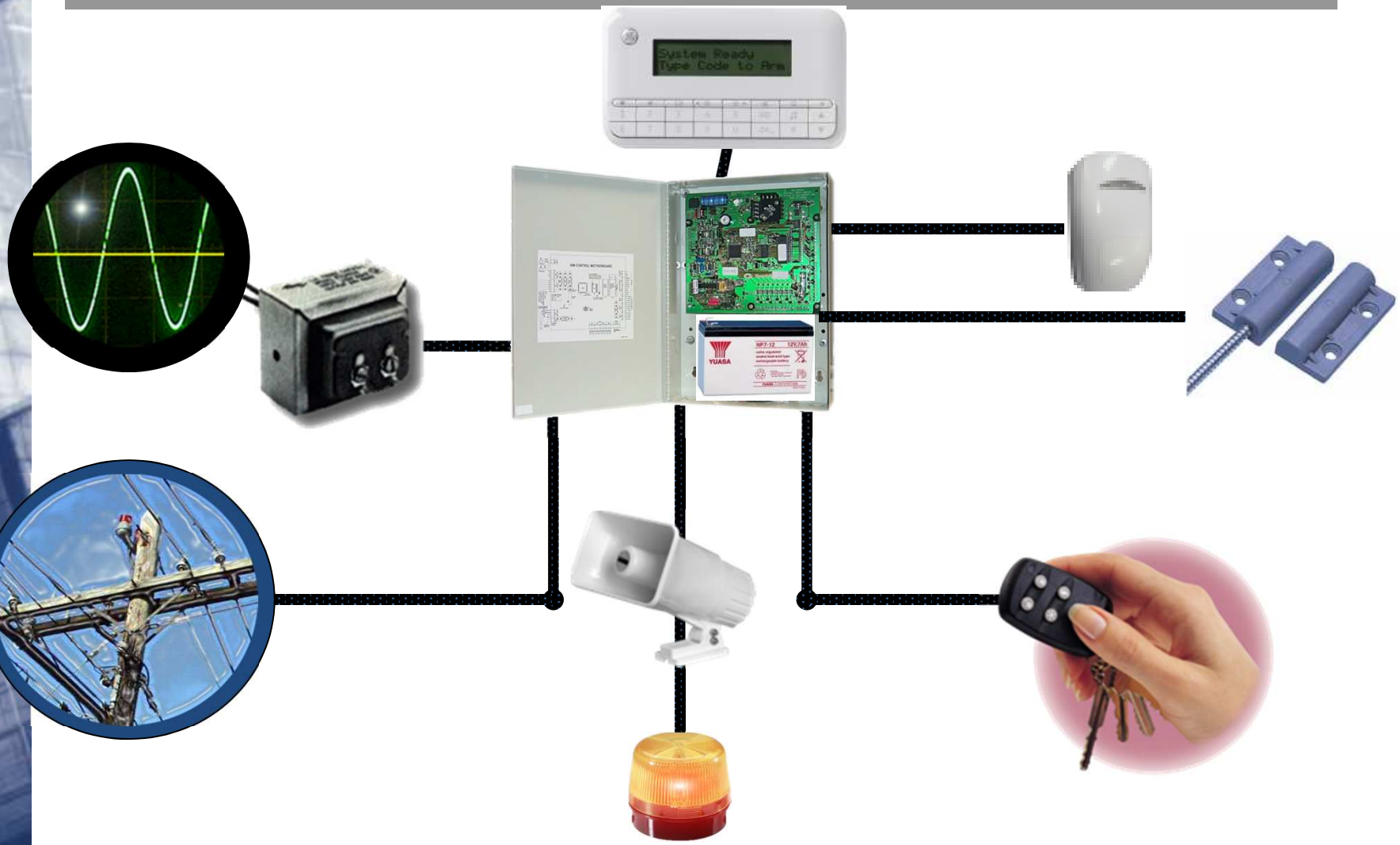
Detección de intrusión

Detección de intrusión

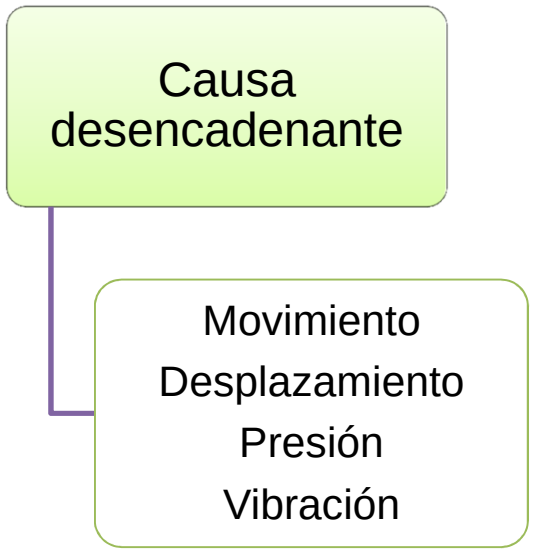
La detección de intrusión se basa en un sistema electrónico que:

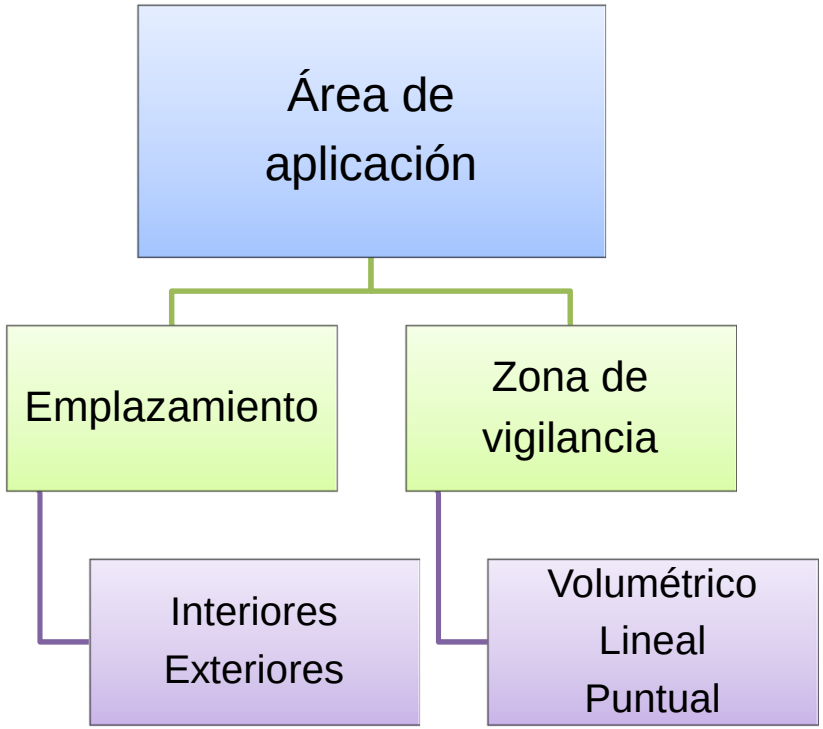
- Detecta entradas no autorizadas cuando el sistema está armado
- Proporciona una indicación audible/visual cuando hay una intrusión
- Transmite a CRA's para posible intervención policial

Detección de intrusión



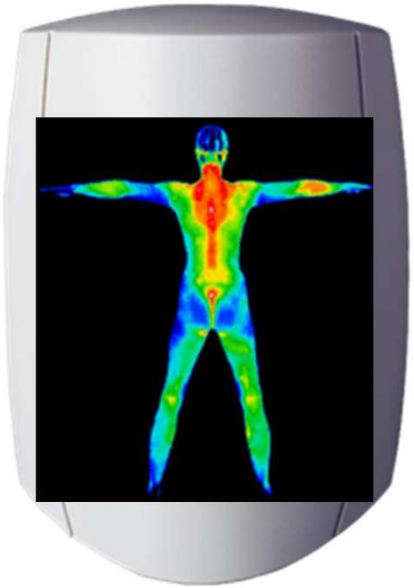
Detección de intrusión (Detectores)



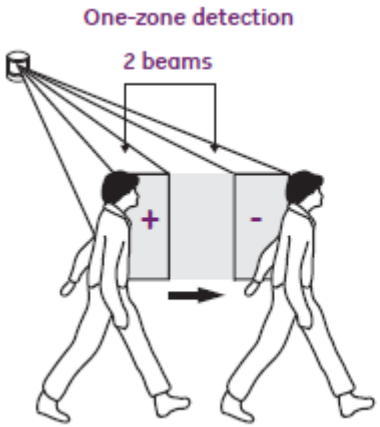


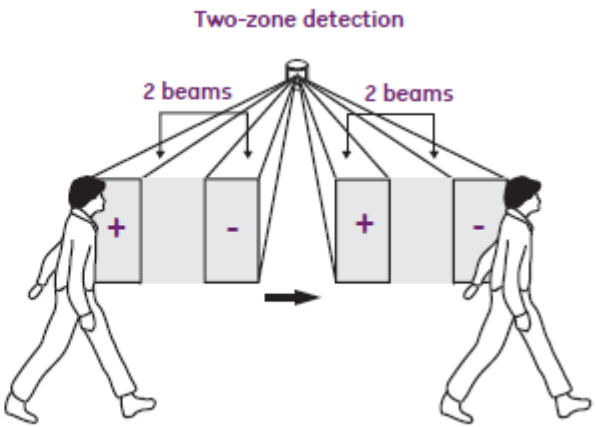
Detección de intrusión (Detectores)

Volumétricos



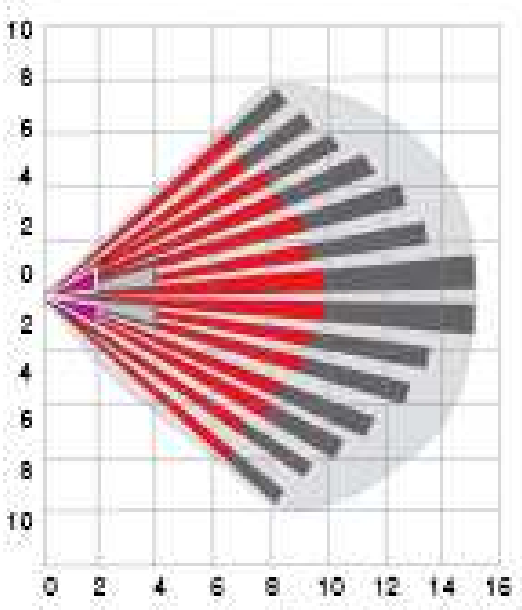
- **Infrarrojo pasivo**
  - Diferencia de temperatura entre áreas



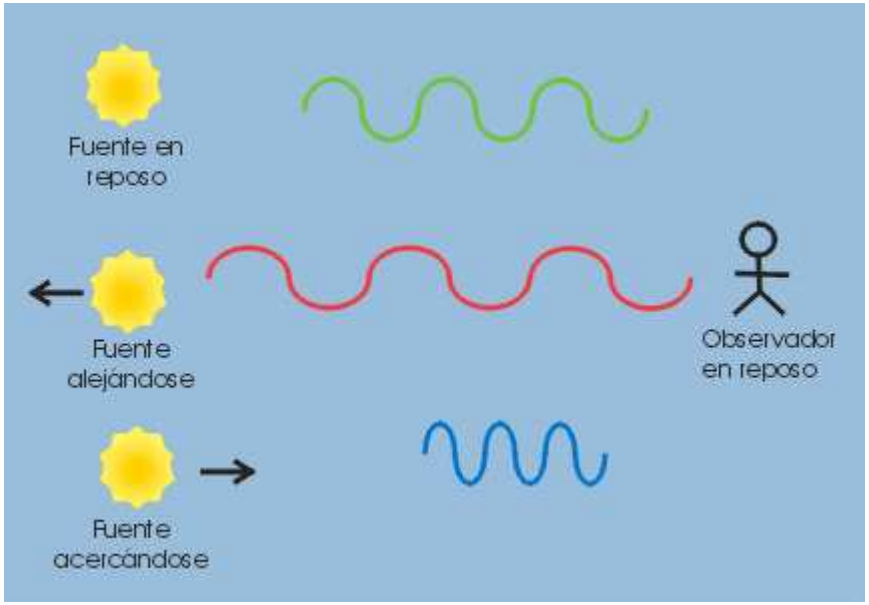


Detección de intrusión (Detectores)

Volumétricos



- Doble tecnología
  - Infrarrojo + Microondas

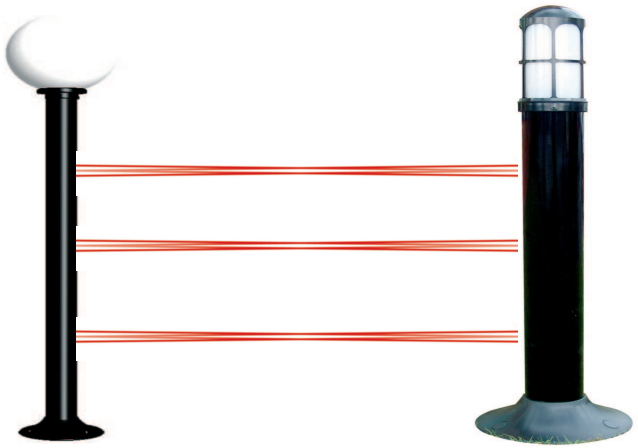


Efecto Doppler

Detección de intrusión (Detectores)

Perimetrales

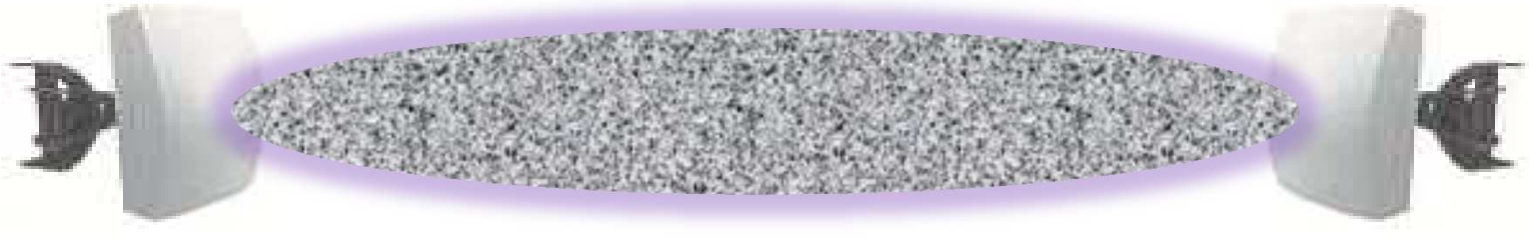
El corte del haz causa la alarma

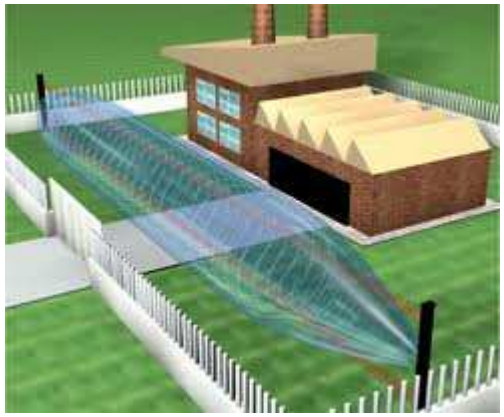


Barreras infrarrojos

Detección de intrusión (Detectores)

Perimetral

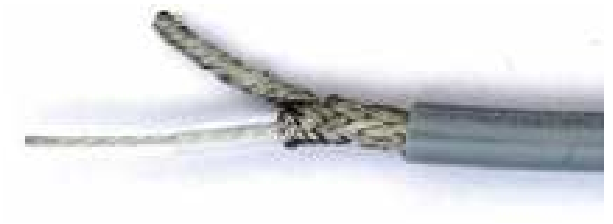




- Microondas

Detección de intrusión (Detectores)

Perimetrales



Cable sensor

Se detecta:

Vibración

Corte

Requiere un buen estado y un buen mantenimiento de la valla

Detección de intrusión (Detectores)

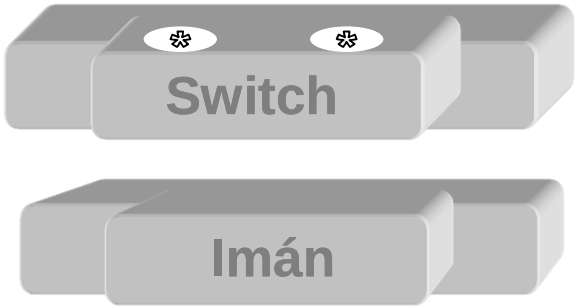
Corte (especiales)

El corte del haz causa la alarma

Fibra óptica

Detección de intrusión (Detectores)

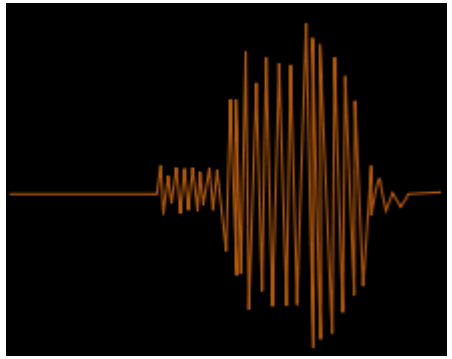
Desplazamiento



El movimiento del imán provoca que el switch se abra causando la alarma

Detección de intrusión (Detectores)

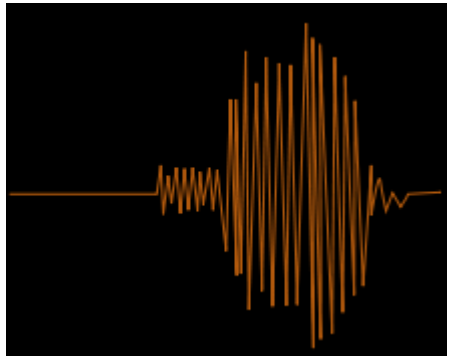
Sísmicos



Detección de la energía transmitida durante el impacto

Detección de intrusión (Detectores)

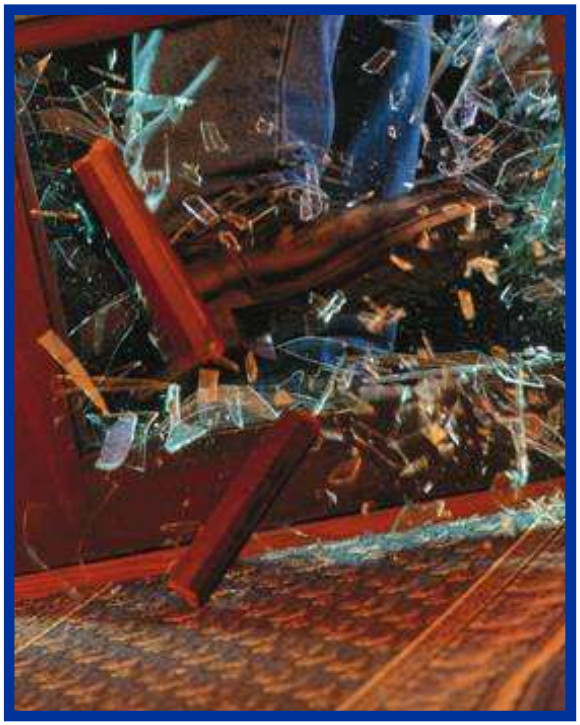
Vibración (Inercial)



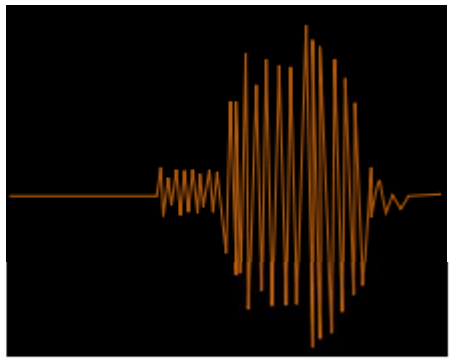
Detección de la energía transmitida durante el impacto

Detección de intrusión (Detectores)

Acústicos



Detección de la frecuencia transmitida durante la rotura del cristal



Detección de intrusión (Detectores)

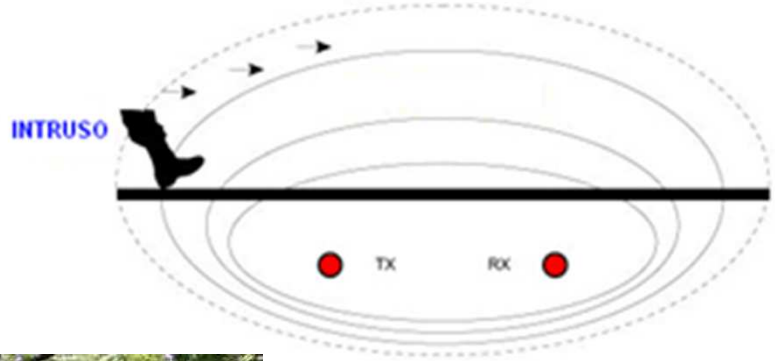
Presión

Alfombra detección pisadas

Detección de intrusión (Detectores)

Enterrados

GPS



Sensor RFC

Campo de Radiofrecuencia

Detección de intrusión (Detectores)

Receptor conectado a la central

© Casmar Electrónica, SA - Confidencial

Detección de intrusión (Pulsadores)

Activados 24h

Detección de intrusión (Sabotajes)

La finalidad del sabotaje es detectar la manipulación no autorizada de los dispositivos del sistema de seguridad

- Detección de apertura
- Retirada del montaje
- Ajuste de la dirección
- Interferencia magnética

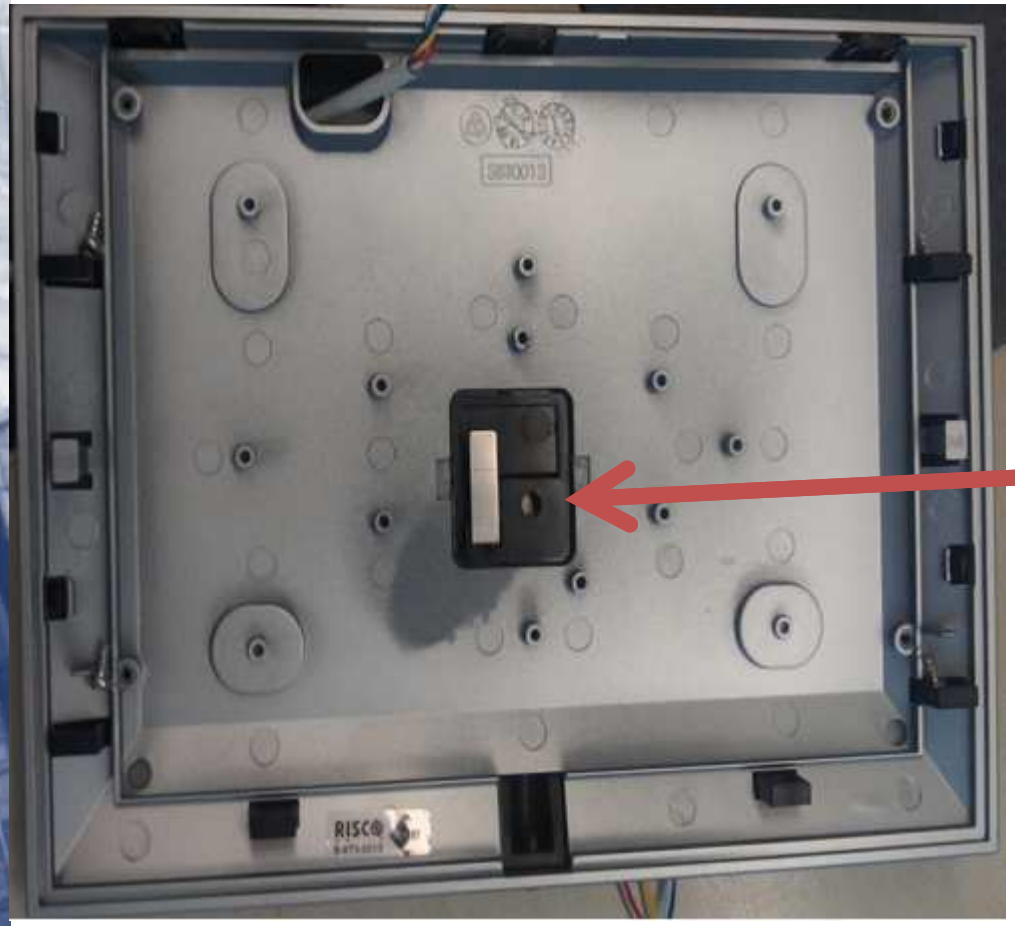
Requisitos Funcionales: Sabotajes

Tipo de Sabotaje a detectar	Grado 2	Grado 3	Grado 4
Apertura medios normales (central, teclado, volumet.,fuente)	✓	✓	✓
Retirada del montaje (central, teclado, volumet., fuente)	Op	✓	✓
Retirada del montaje elementos vía radio	✓	✓	✓
Penetración (central , teclado, transm. ext., sirena, fuente) (a)	Op	Op	✓
Volumétrico: ajuste de la orientación (b)	Op	✓	✓
Magnético: resistencia para acceder al interior	✓	✓	✓
Magnético: retirada del montaje	Op	Op	✓
Magnético: interferencia del campo magnético	Op	✓	✓

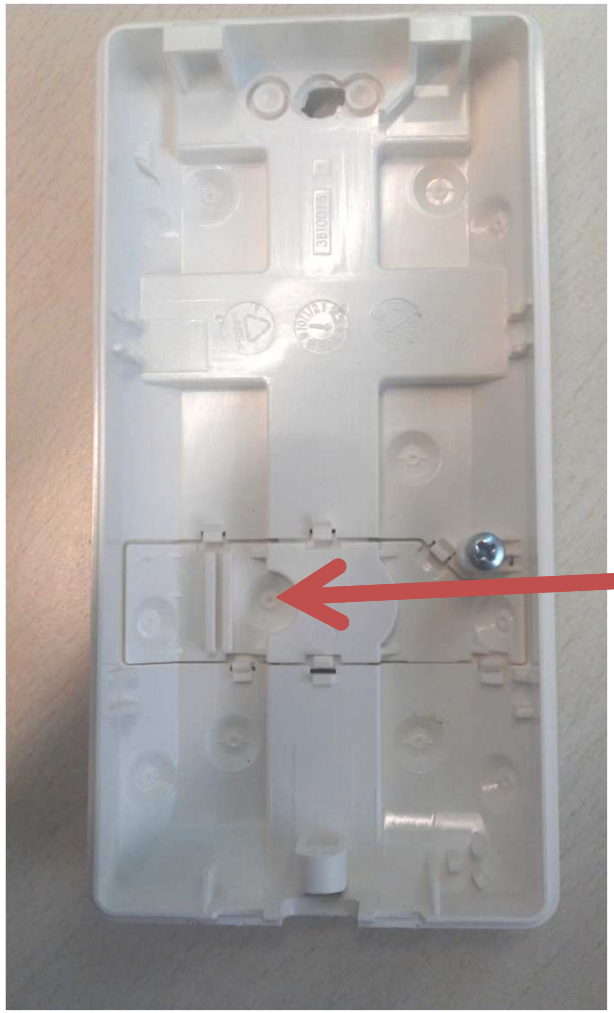
(a) Cuando están situados fuera del área vigilada
(b) Cuando sea posible

© Casmar Electrónica, SA - Confidencial

Sabotajes:
Retirada del montaje

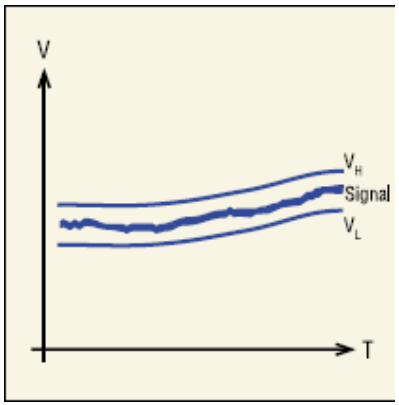


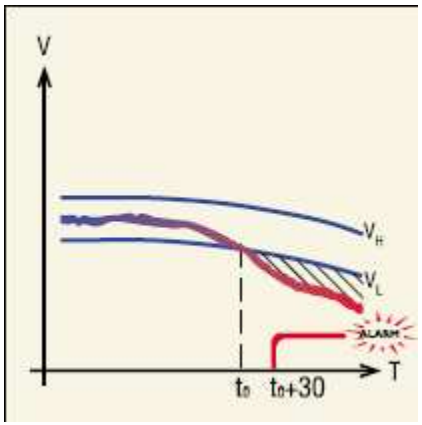
Sabotajes: Retirada del montaje

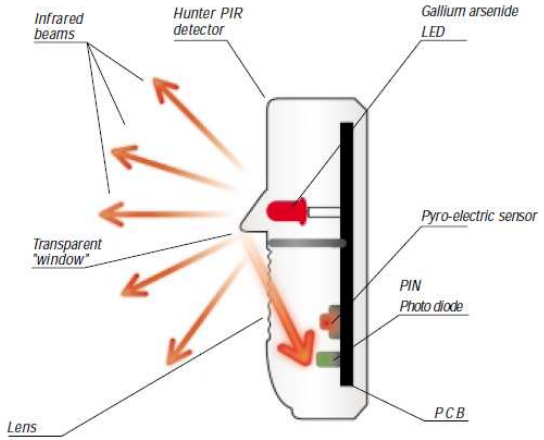


Detección de intrusión (Sabotajes)

- Antimasking



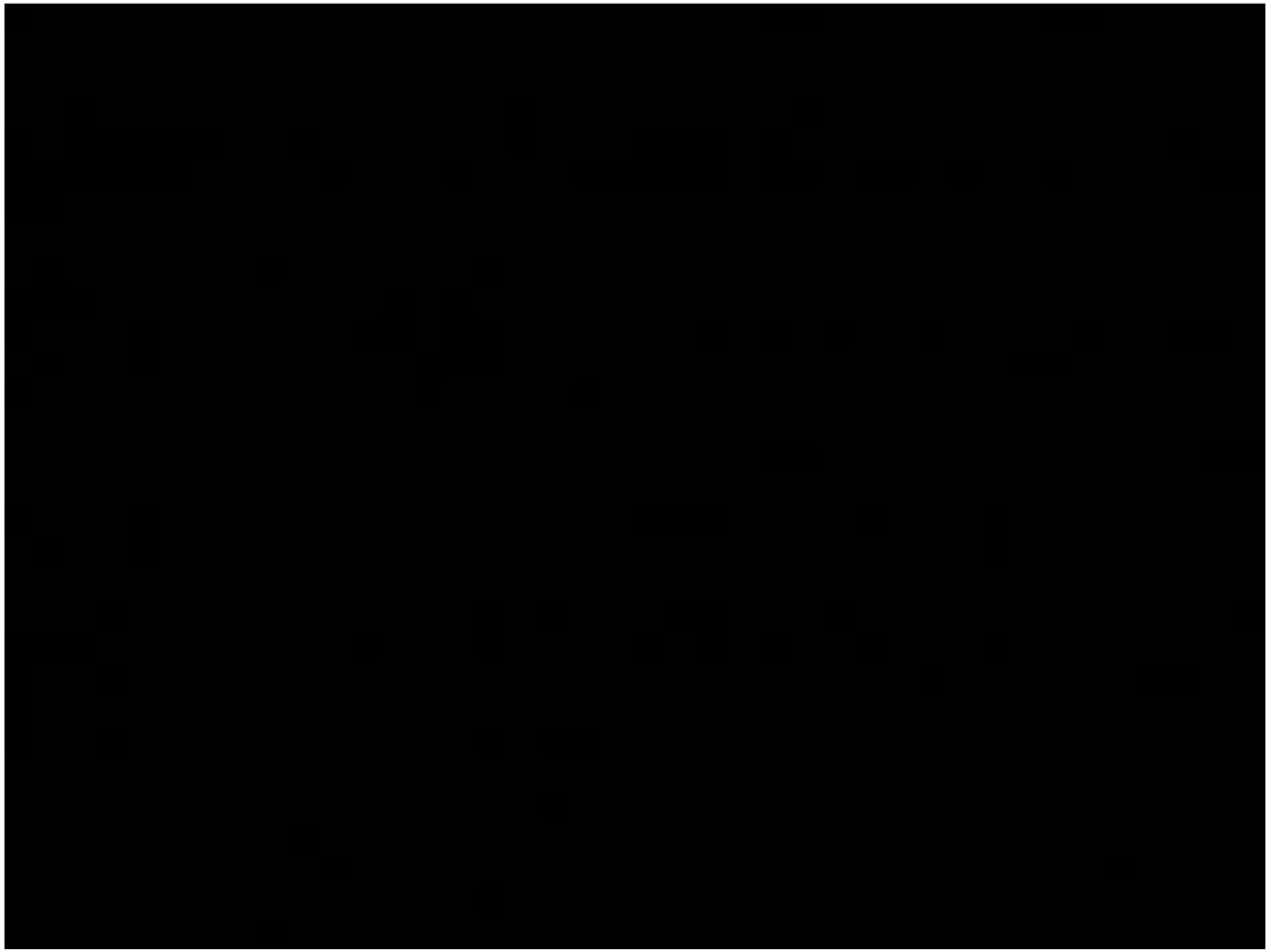




© Casmar Electrónica, SA - Confidencial

Función Anti-Camuflaje

- Anticloak



Función Anti-Camuflaje

Imagen Térmica
Intruso Normal

Imagen Térmica
Intruso Apantallado

- **Función Anti-Camuflaje mejorada**
  - Diseñado para detectar intrusos con una diferencia muy BAJA de temperatura respecto al ambiente
  - Analiza y memoriza la actividad “normal” del ambiente (sin intruso)
  - Realiza avanzados análisis de actividad (con intruso) y compara con la actividad “normal” del ambiente
  - Nunca desconecta el canal PIR
- **Ventajas**
  - Detecta intrusos camuflados que los detectores PIR y DT normales no pueden
  - Minimiza la pérdida del rango de cobertura en temperaturas ambientes similares a las del intruso
  - Mantiene la inmunidad a las falsas alarmas de un DT

Guardall

Requisitos Funcionales: Opciones de notificación de alarmas

	Grado 2				Grado 3				Grado 4			
	A	B	C	D	A	B	C	D	A	B	C	D
Sirena sin batería	2	Op	Op	Op	2	Op	Op	Op	2	Op	Op	Op
Sirena auto-alimentada	Op	1	Op	Op	Op	1	Op	Op	Op	1	Op	Op
Transmisión principal	ATS2	ATS2	ATS2	ATS3	ATS4	ATS4	ATS4	ATS5	ATS5	ATS5	ATS5	ATS6
Transmisión secundaria	Op	Op	ATS1	Op	Op	Op	ATS3	Op	Op	Op	ATS4	Op

Detección de intrusión (Notificación)

Sirenas

- Efecto disuasorio
- Avisa de una condición de alarma

Reglamentación local

Lanzadestellos

- Flashes estroboscópicos
- Permite localizar rápidamente una condición de alarma

Detección de intrusión (Notificación)

Transmisores

- Envío de mensajes a CRA
- Identificación mediante código abonado
- Identificación tipo de alarma

Tecnologías de transmisión

- RTC
- GSM
- IP
- GPRS

Detección de intrusión (Notificación)

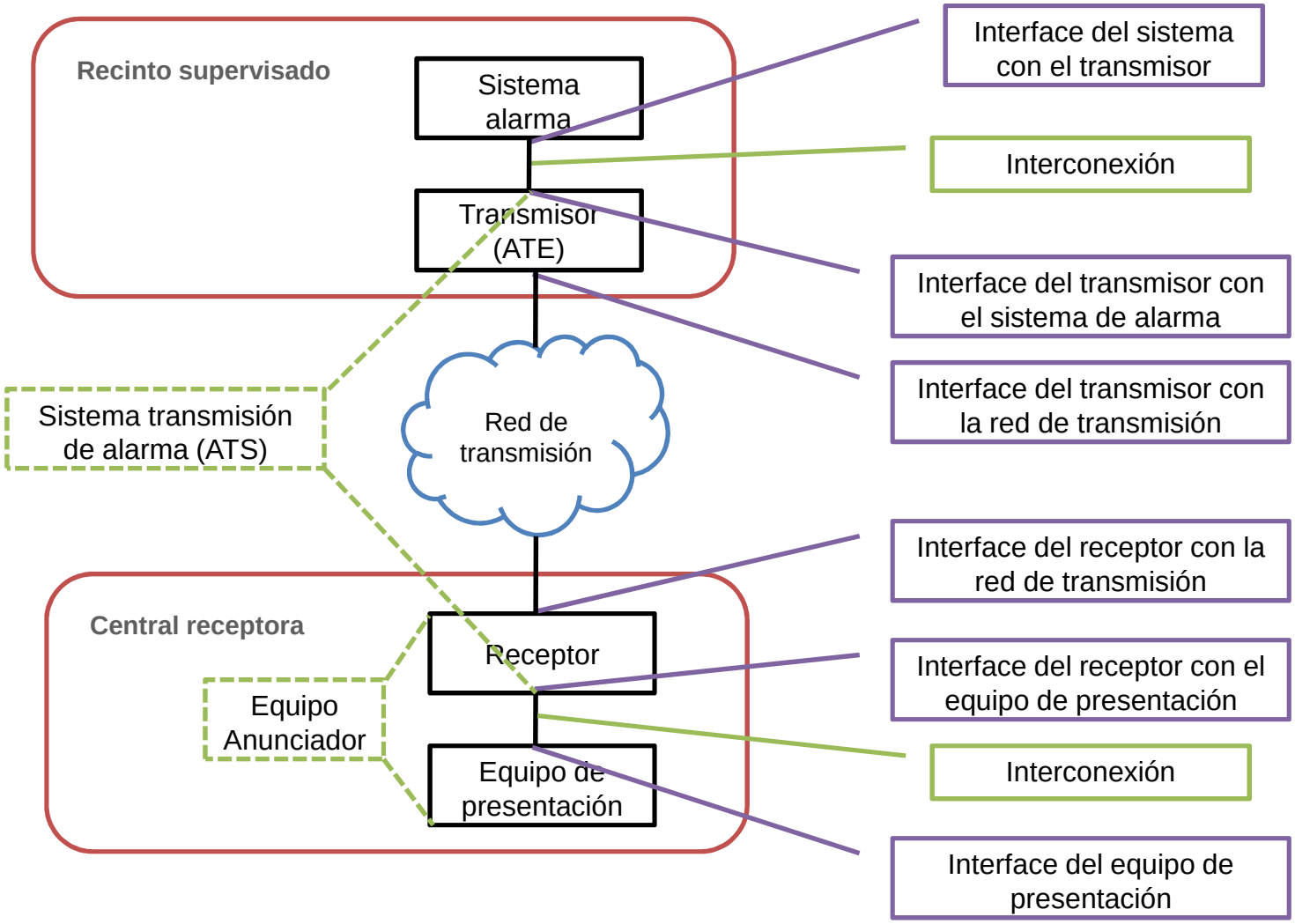
Receptoras

- Recepción señales de diferentes abonados
- Diferentes formatos de transmisión
- Supervisión de los enlaces de transmisión

Tecnologías soportadas

- ANALÓGICA: RTC-GSM
- DIGITAL: ADSL, GPRS

Requisitos Funcionales: Notificación Sistema Transmisión



Requisitos Funcionales: Notificación Características Sistema Transmisión

Las características de funcionamiento de un sistema de transmisión se evalúan en base a los siguientes criterios:

Nivel ATS:

El tiempo de transmisión	✓
La seguridad de la señalización	✓
El tiempo de información (tiempo de supervisión)	✓

Más:

La disponibilidad	✓

Requisitos Funcionales: Notificación (sistema transmisión)

Nivel	Tiempo de transmisión		Tiempo de información (Auto-Test o Polling)	Seguridad de la señalización	
	Media aritmética de las transmisiones	Valor Máximo		Seguridad sustitución	Seguridad información
ATS1	120”	480”	25h	Sin medidas	Sin medidas
ATS2	60”	120”	25h	Sin medidas	Sin medidas
ATS3	60”	120”	25h	Detección identidad falsa	Evita lectura
ATS4	60”	120”	300’	Detección identidad falsa	Evita modificación
ATS5	20”	60”	180”	Encriptación identidad o Autentificación	Evita lectura y modificación
ATS6	10”	20”	20”	Encriptación identidad o Autentificación	Evita lectura y modificación

© Casmar Electrónica, SA - Confidencial

Proyecto de instalación

Conforme norma UNE-CLC/TS50131-7

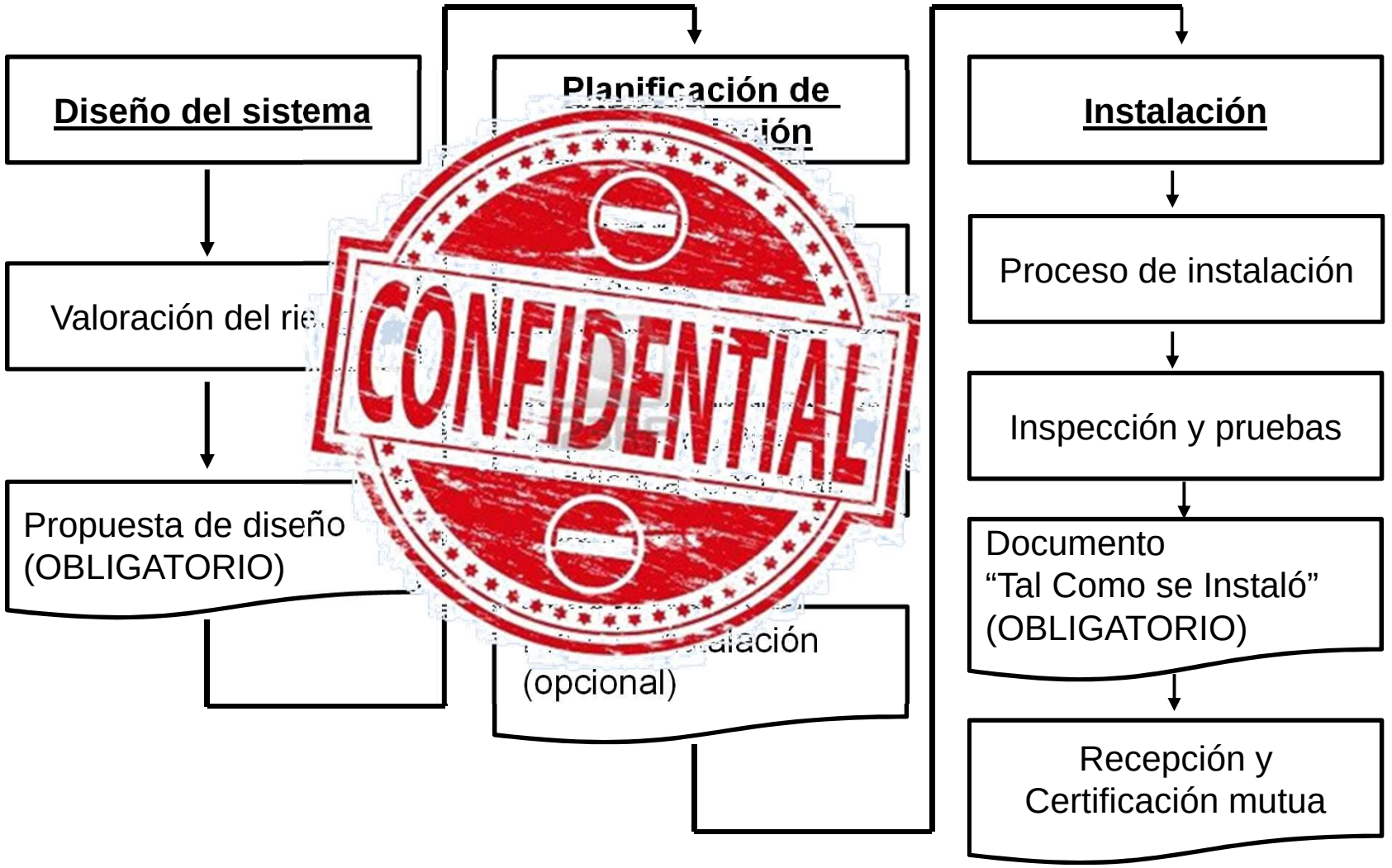
- Requisitos mínimos
- Se determinan características de diseño e instalación en función de:
  - Naturaleza del activo protegido
  - Valor de su contenido
  - Nivel de riesgo de intrusión
  - Amenaza para el personal
  - ……

Objetivos

- Prevenir y proteger
- Minimizar falsas alarmas
- Colaboración del usuario

Evaluación de riesgos

Aplicación de la norma 50131-7 conforme a las Ord. Ministeriales



Diseño: supervisión mínima

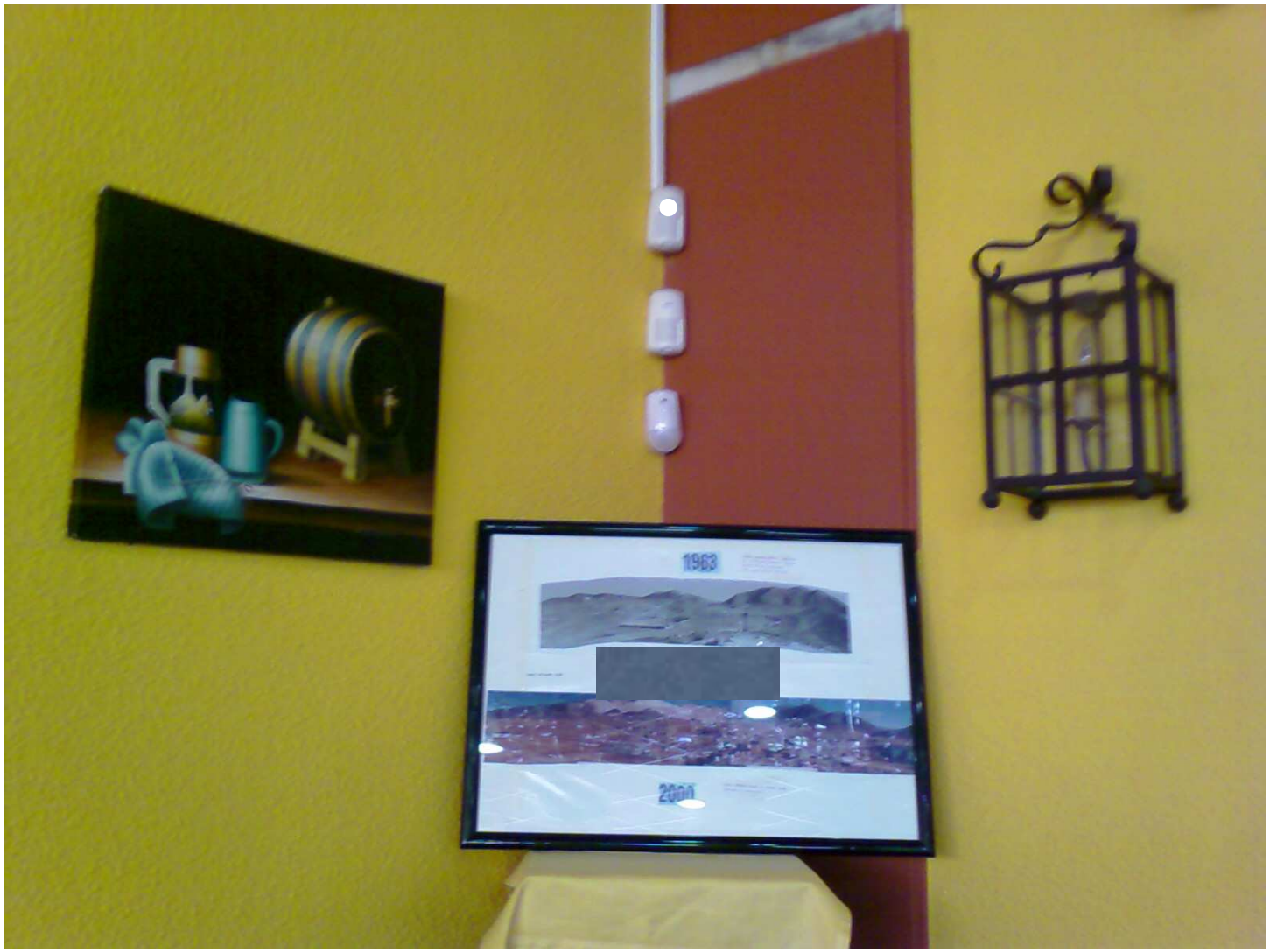
Guía para:

- Diseñador
- Cliente

Se debe basar en:

- El análisis de riesgo

Ejemplo de supervisión mínima



Resumen de Documentación para el Cliente

- **Proyecto (Propuesta de diseño)**

- **Manuales del Sistema**
  - Manual de Instalación “Tal como se instaló” (As Built)
    - ✓ Planos, ubicaciones, coberturas, cableados,...
    - ✓ Detalle de certificados de homologación de materiales
  - Manual de uso
    - ✓ Cómo usar el sistema
    - ✓ Mantenimiento por parte del usuario
    - ✓ Averías frecuentes

- **Contratos**
  - de Instalación
  - de mantenimiento
  - de conexión a CRA
  - (servicio de acuda)

- **Certificados**
  - de instalación
  - de conexión a CRA
  - de aceptación por parte del usuario del sistema de alarma
    - ✓ del funcionamiento del servicio
    - ✓ de las características técnicas y funcionales del sistema
    - ✓ de información las responsabilidades
    - ✓ de formación al usuario

- **Libro catálogo y de revisiones**

Videovigilancia

Videovigilancia (Concepto)

Un circuito cerrado de televisión es, básicamente:

Es, también, una herramienta muy potente de gestión del riesgo

Videovigilancia (finalidad)

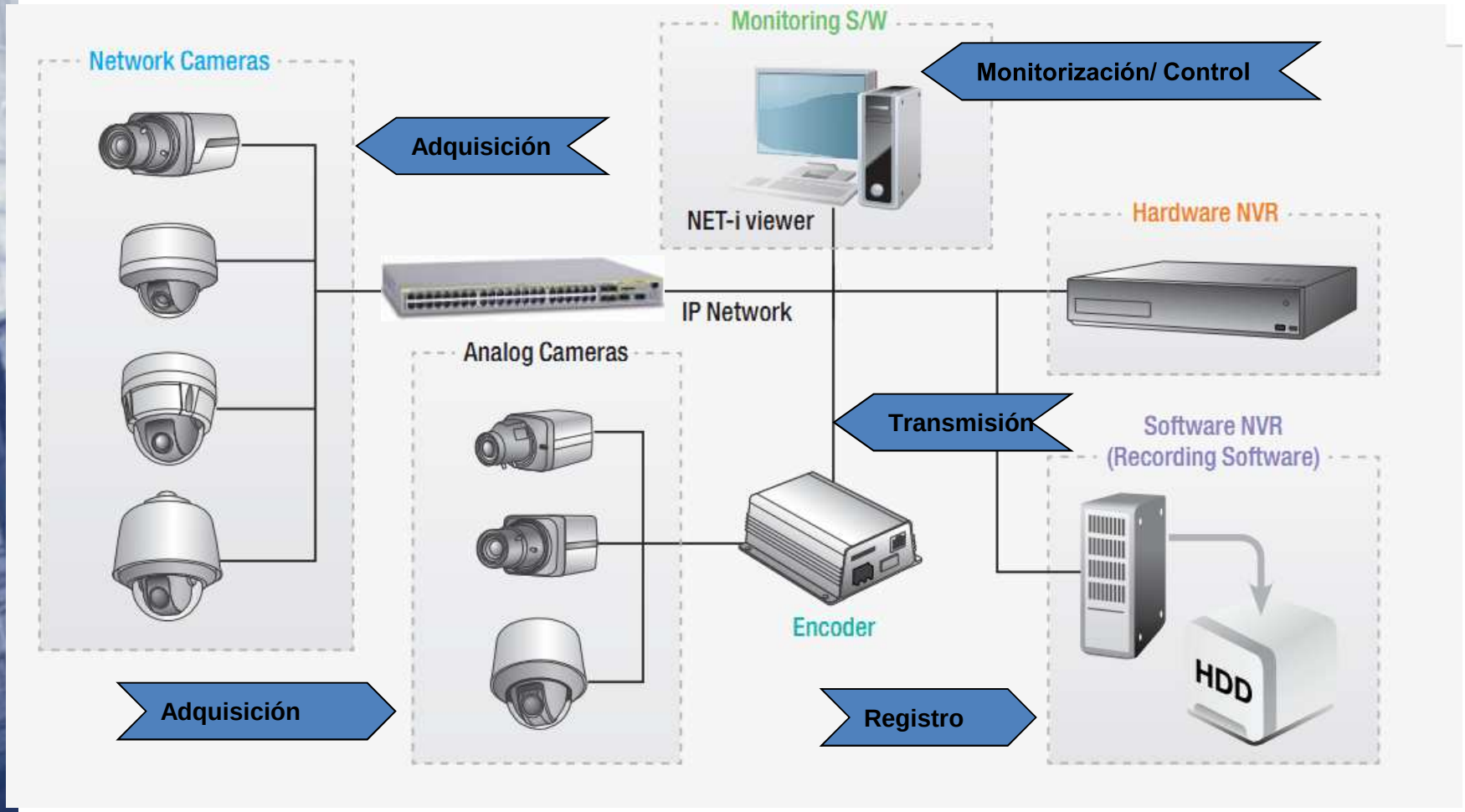
Proactiva

- Permite monitorear la escena a proteger y lograr una rápida reacción en caso de necesidad

Reactiva

- En caso de que ocurra algún incidente, el sistema proporciona datos para poder investigar

ELEMENTOS SISTEMA CCTV



Toma de decisiones

- ✓ **Definir el objetivo de videovigilancia:**
  - visión amplia o,
  - nivel de detalle más elevado.
- ✓ **Entorno interior o exterior.**
- ✓ **Iluminación**
- ✓ **Calidad de imagen.**
- ✓ **Resolución.**
- ✓ **Medio de transmisión.**
- ✓ **Grabación**
- ✓ **Visualización**

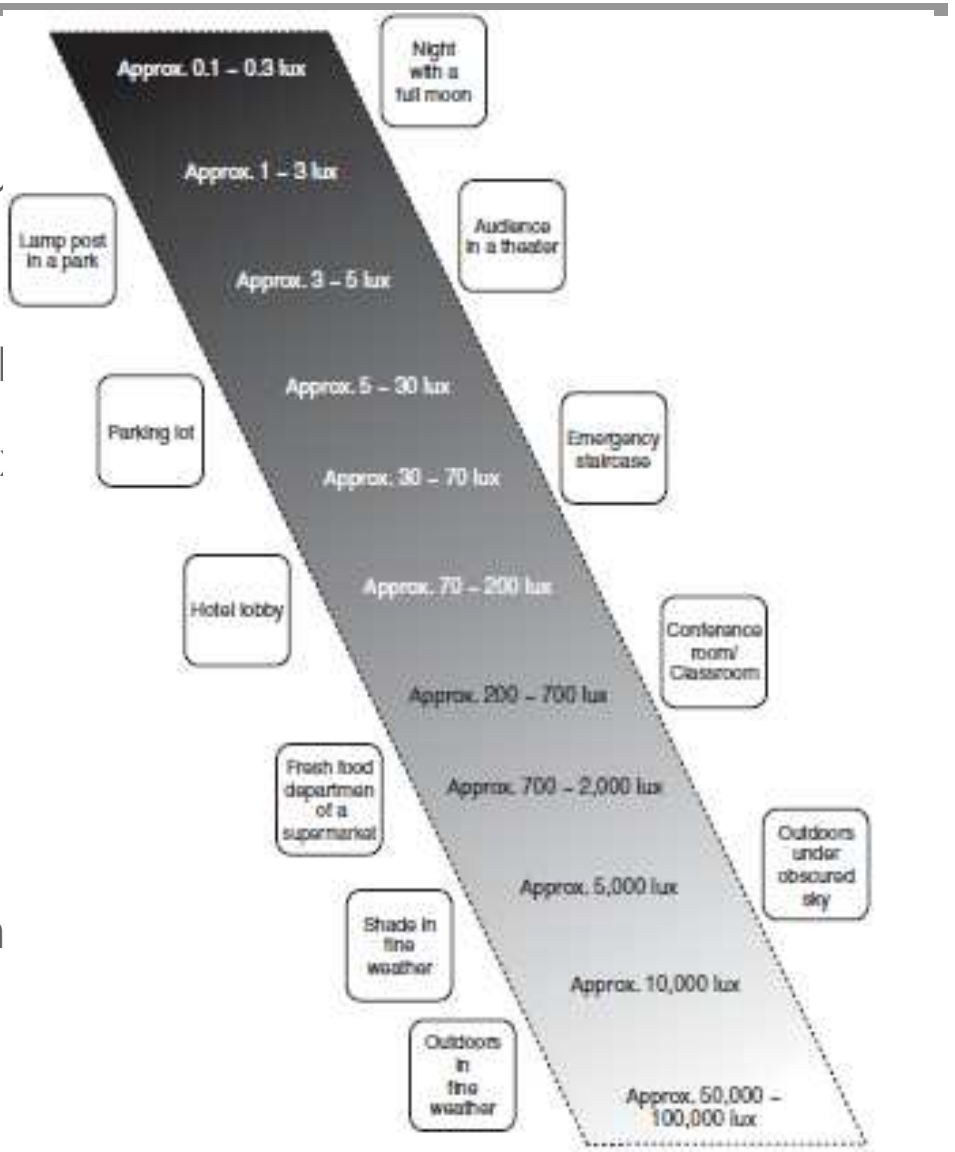
Tipos de cámara

En función de su movimiento

- **Fijas**
- **Domo (PTZ)**
  - **Preset's**
  - **E-flip**
  - **Auto flip**

Sensibilidad luminosa

- Las cámaras requieren ci
  de luminosidad para produ
  de calidad.
- Se mide en Lux (footcandl
- Para condiciones de luz e
  existen cámaras con LEDs
  cámaras anti-reflejos.
- En condiciones de baja lu
  el ruido (dB) de la señal de
  más evidente (especialmen
  cámaras estándar a color).

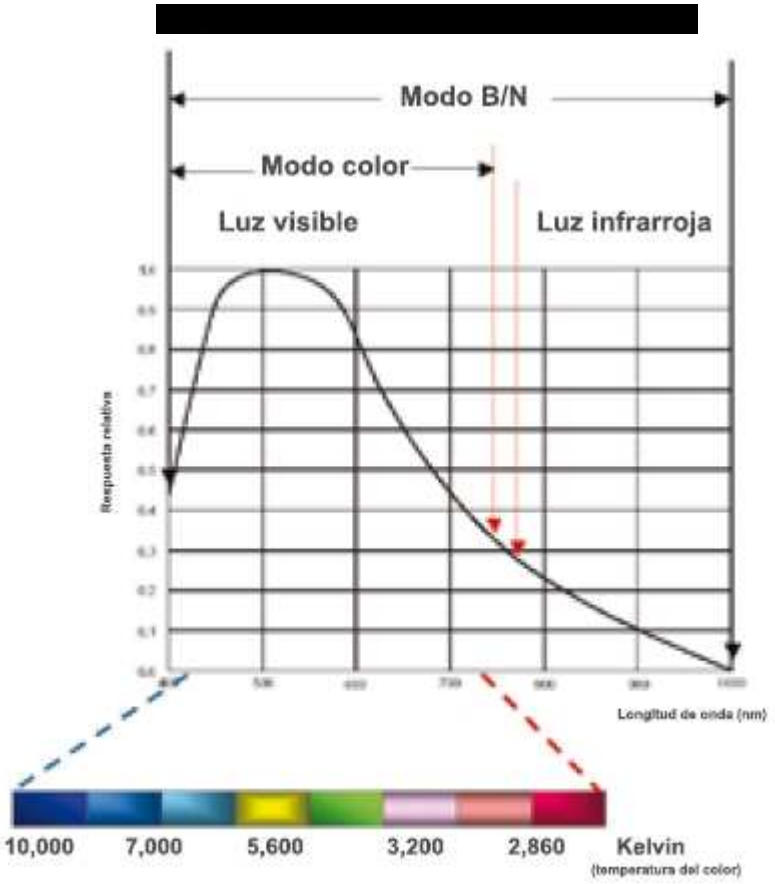


Tipos de cámara

En función de la imagen

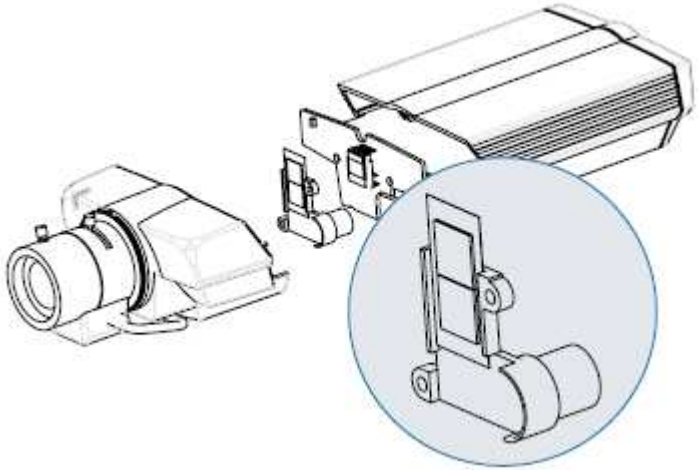
- Color
- Blanco/negro

Día/Noche



Tipos de cámara

Conmutación Día/Noche



Día

Noche

BLC - Wide Dynamic Range

WDR (Rango Amplio Dinámico): Para imágenes más detalladas bajo condiciones de luz variables.

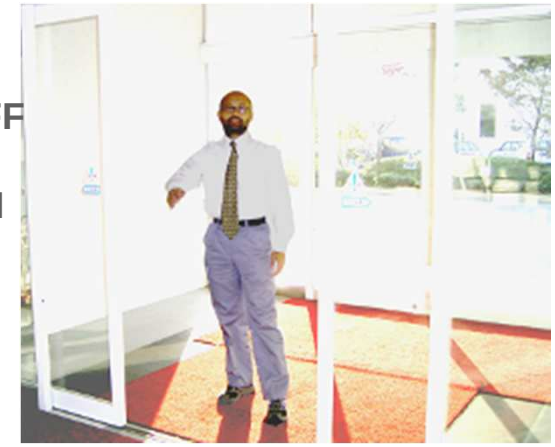
→ Captura a 2 vel. de obturador (1/50) y Alta vel. para combinar ambas capturas en una sola imagen detallada sin sombras ni deslumbramientos

WDR:OFF

BLC: OFF

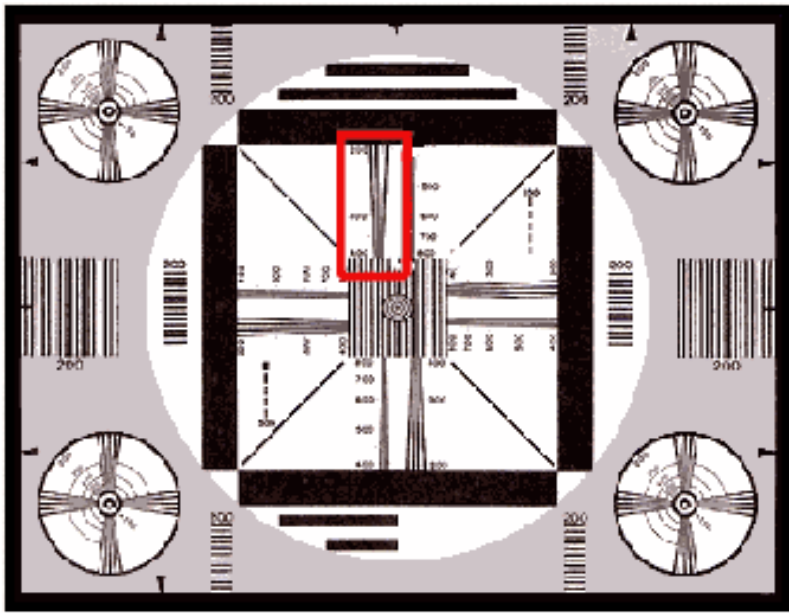
WDR:OFF

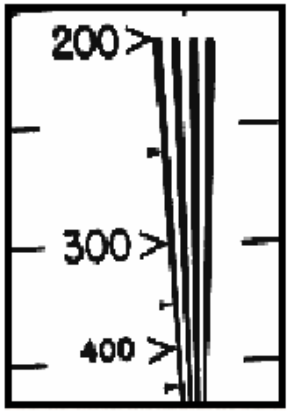
BLC: ON



Imágenes con función Wide Dynamic activa.

Resolución



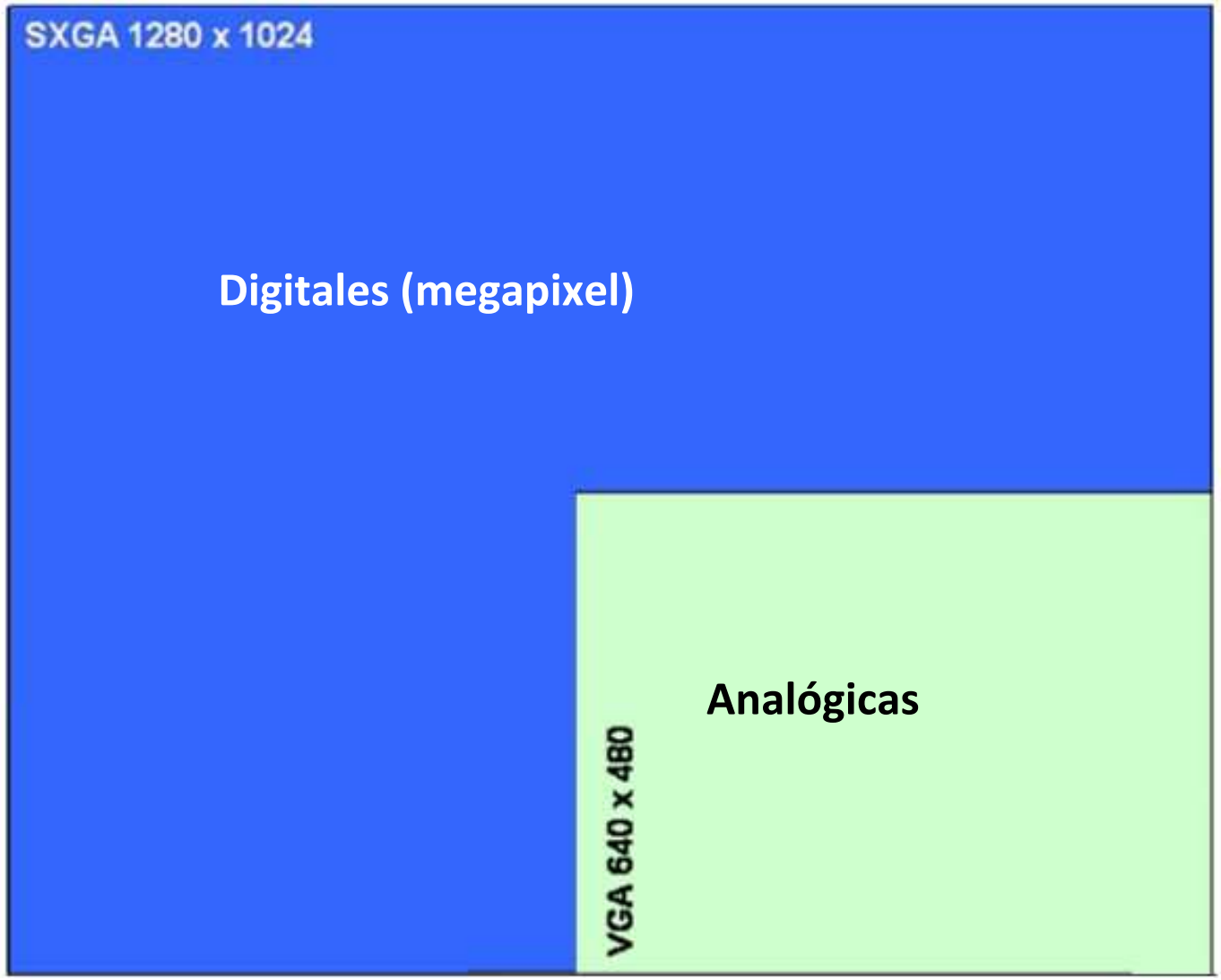


- La resolución es una medida de capacidad de la cámara para reproducir detalles.
- A mayor resolución tenemos imágenes más definidas
- Se mide en TVL según un patrón de prueba.

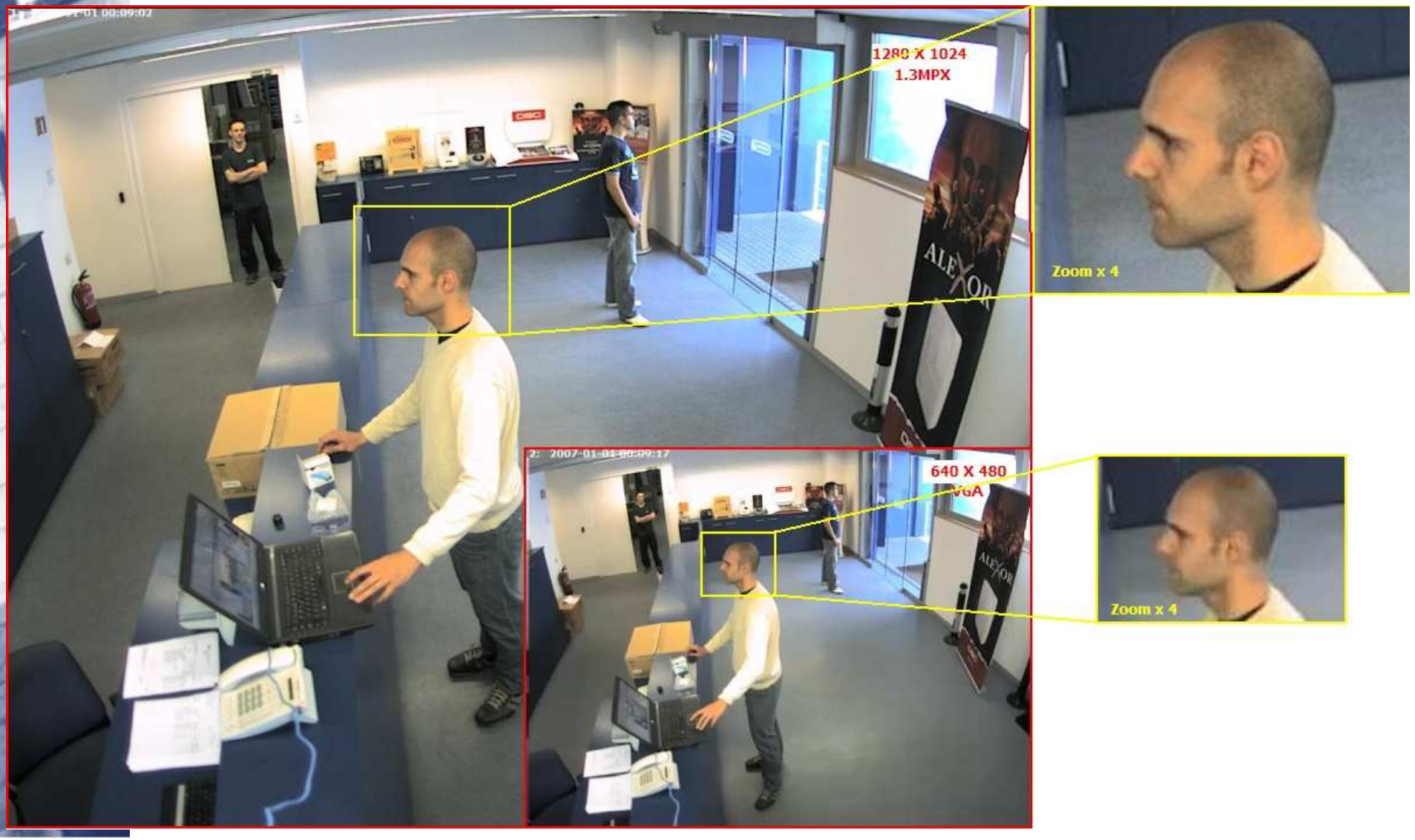
<u>Resolución Analógica:</u>

❖Estándar (Baja):
330 TVL
❖Media:
420 - 450 TVL
❖ Alta:
480 TVL – 550 TVL
> 600 TVL (Súper Alta)

Cámaras Megapixel



Cámaras Megapixel



Ópticas

En función de su óptica

- Fijas
- Varifocales
  - Manuales
  - Automáticas

En función de las condiciones de iluminación

- Iris fijo
- Iris manual
- Autoiris

Distancias focales

Distancias Focales Comunes:

(90º - 36º) → Aplicaciones en interiores
(97º- 26º) → Visión gran angular o combinación interior- exterior
(53º - 5,5º) → Aplicaciones en exterior

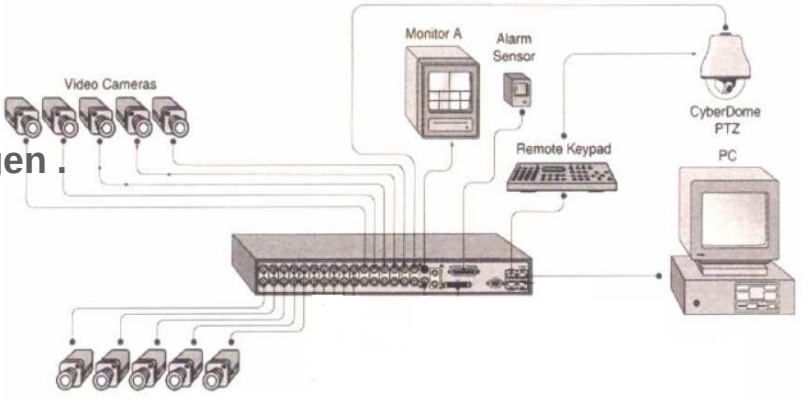
Enfoque

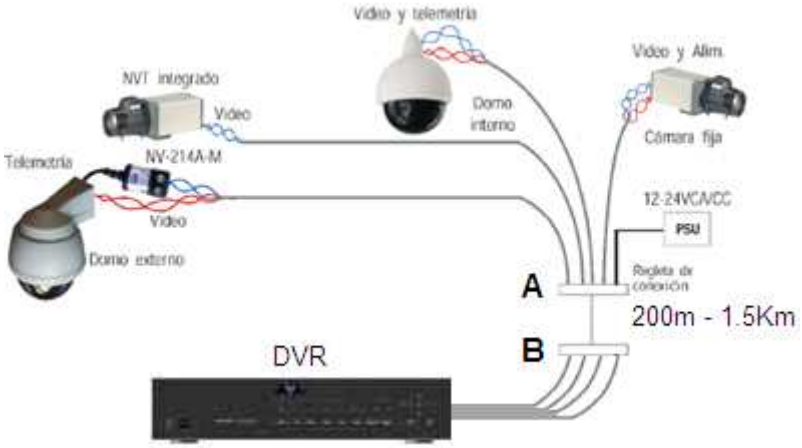
Foco o enfoque:

Es la herramienta del lente que nos permite ajustar la nitidez y los detalles de la imagen observada en el monitor

CCTV - TRANSMISIÓN

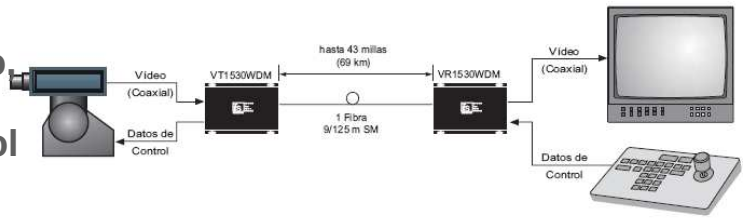
Coaxial **se recomienda un blindaje de cobre entre 75Ohm a 95, se puede alcanzar de 200m-300m, Cable uno por cámara , sensible al tipo de conectores desmejorando la calidad de la imagen . Se recomienda para aplicaciones pequeñas.**



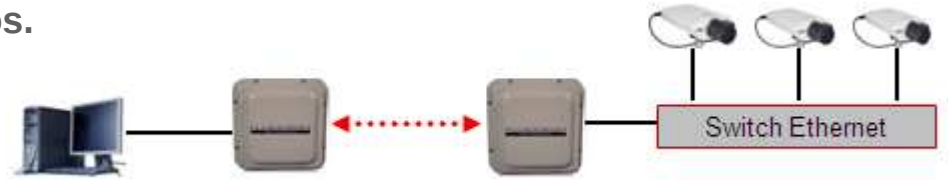


UTP**: Mano de obra reducido, distancia de trasmisión de 1,6KM. Puede ser amplificado o pasivo.**

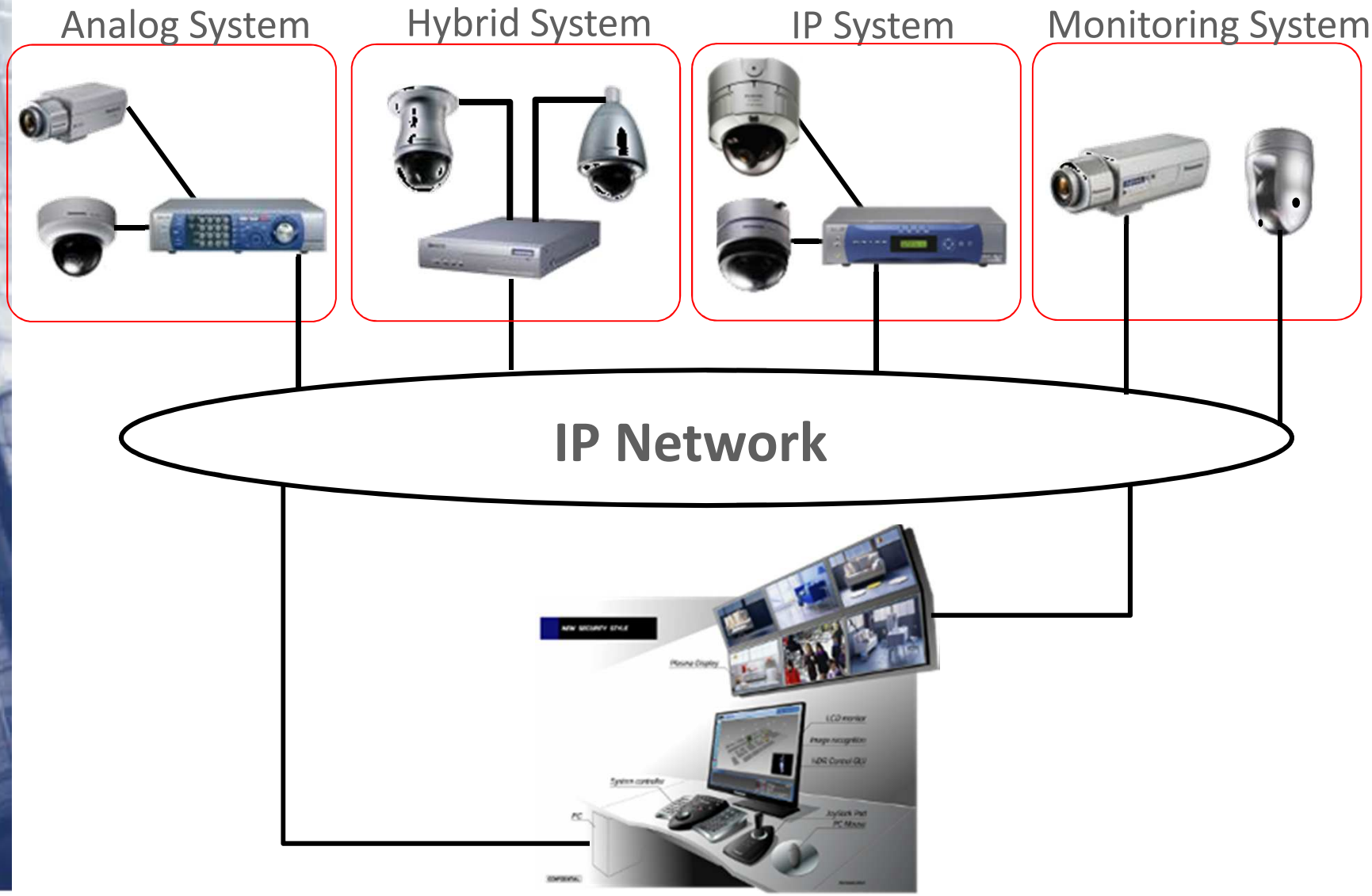
Fibra óptica: **Proporciona una alta inmunidad al ruido distancia sin amplificador a 49 Km. Los equipos son PLUG & PLAY, formato tipo rack, permiten control RS485 por la misma fibra.**



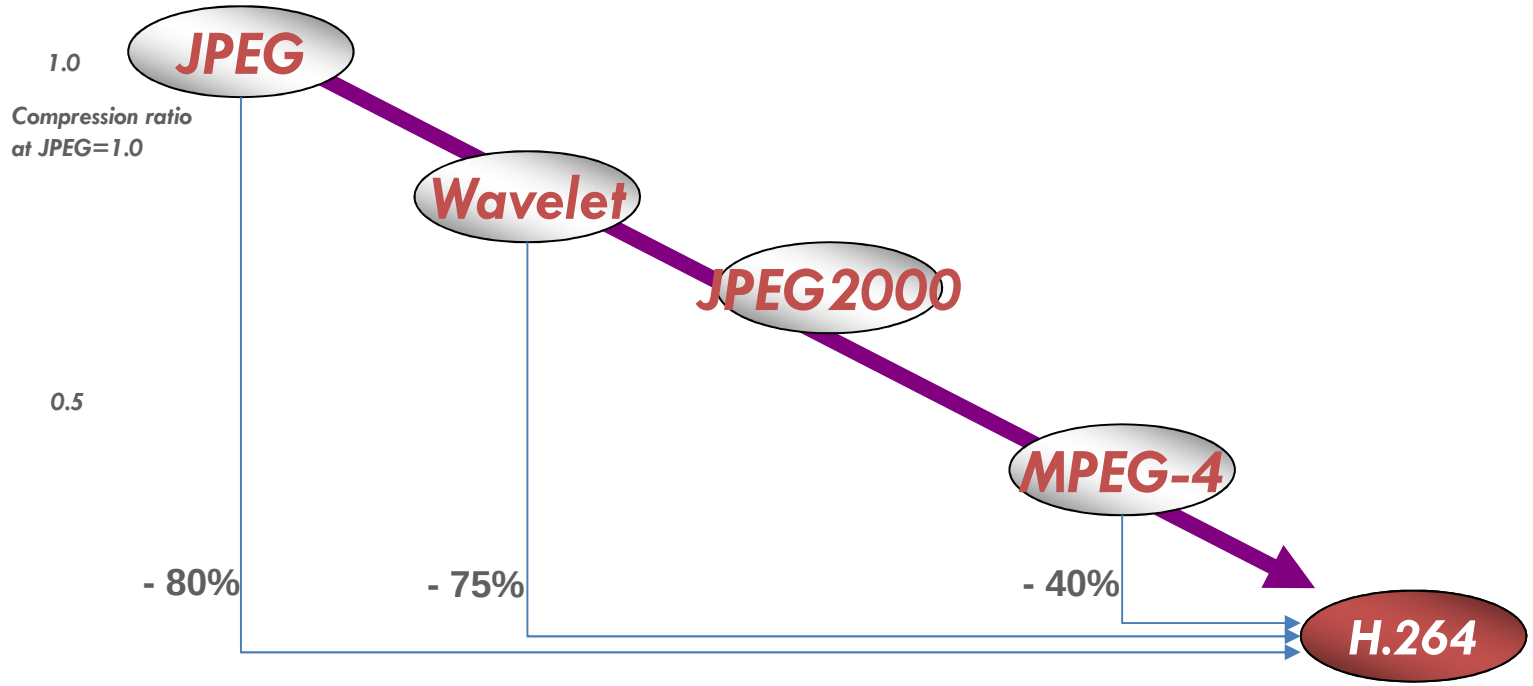
Inalámbrico: **Transmisor de señal Ethernet vía radio para exterior con protección IP68 y antena direccional integrada. Sólo para cámaras IP, las distancias varían según lo definido por los parámetros inalámbricos.**



Instalaciones Híbridas



Grabación
Comparativa compresión



*Figures in this page are subject to change without notice

La compresión H.264 reduce el ancho de banda y el almacenamiento hasta un 40% comparándolo con una compresión MPEG-4

Grabación

Problema de conexión

Grabación

Reestablecimiento
de la conexión
Panasonic
SD
2GB
Transferencia desde la tarjeta SD
Grabador
o
FTP Server

Grabación

La función cliente FTP habilita transferencias de imágenes en tiempo real a un servidor FTP. Las imágenes correspondientes a alarmas también son transferidas

Grabación

- Altas Prestaciones para grabación en Red
- Gran capacidad de almacenamiento
- Mantenimiento fácil
- Operación Simple
- Seguro y fiable
- Capacidad Megapixel
- H.264 High Profile

Visualización

- Tecnologías PLASMA, LCD y LED’s
- Diferentes tamaños de pantallas
- Diferentes configuraciones

Visualización

- Soporte PDA y Smart Phone & i-Phone
- Video/audio directo remoto
- Funciones remotas basadas en web
- Playback remoto
- Control IO/PTZ remoto
- Backup remoto
- Soporta 3GPP streaming para telefonía móvil

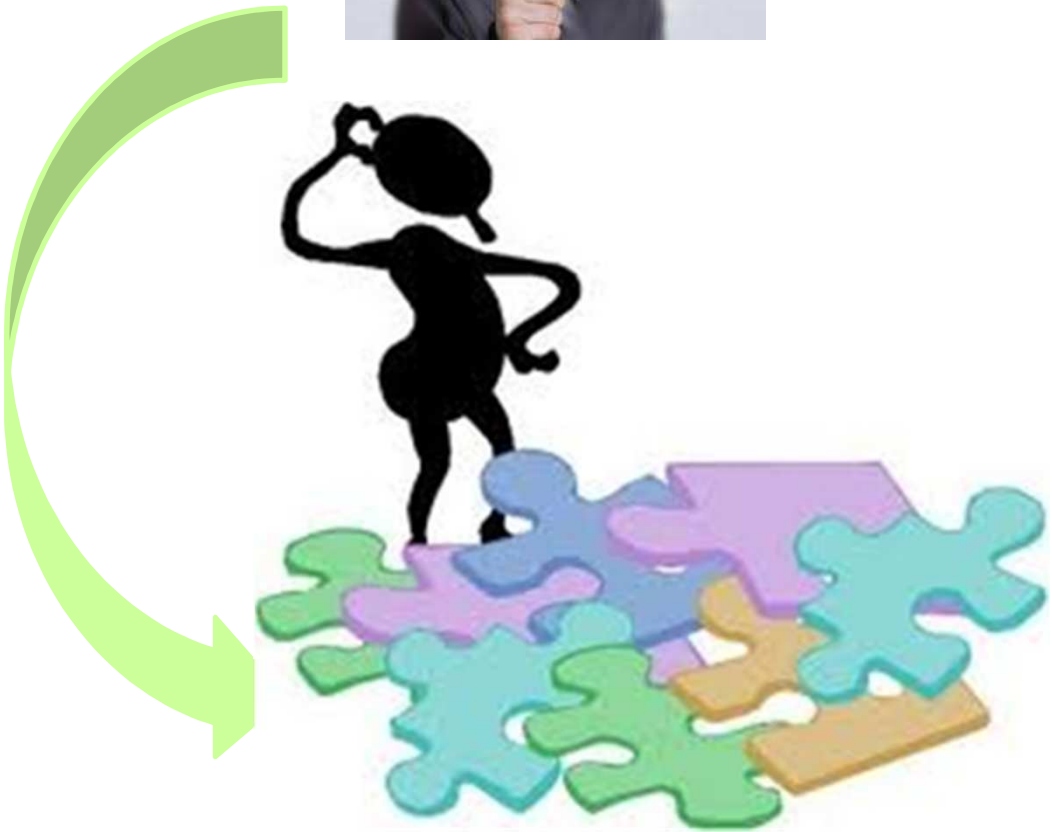
Contexto Legislativo

Protección de derechos fundamentales de la persona

- **Ley 15/1999 orgánica de protección de datos**
- **Real decreto 1720/2007 de 21 de diciembre**
- **Instrucción 1/2006 de 12 de diciembre (VIDEOVIGILANCIA)**

Planteamiento

Normativa



eureka®

Videovigilancia (privacidad)

Imagen es un dato de carácter personal:

- Identifica y hace identificable a personas

Aplica la Ley Orgánica de protección de datos de carácter personal (LOPD)

Instrucción videovigilancia 1/2006

Principios de protección de datos

Aquellas personas o entidades que instalen sistemas de videovigilancia para captar o tratar imágenes en las que puedan aparecer personas identificables, deben observar ciertos principios generales de actuación de conformidad con lo dispuesto en la legislación de protección de datos y de las circulares y resoluciones de la Agencia Española de Protección de Datos (AEPD)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

apdcat
Autoritat Catalana de Protecció de Dades

Agencia de Protección de Datos de la Comunidad de Madrid

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

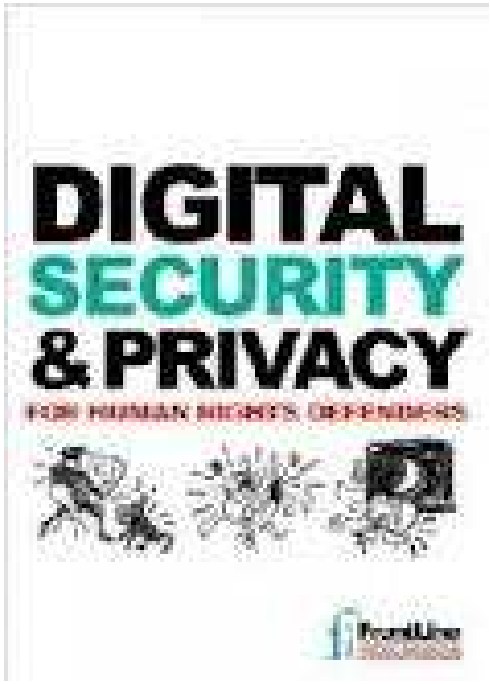
Derechos del propietario de los datos

DERECHO A SER INFORMADO

1. Carteles
2. Impresos informativos

EJERCICIO DERECHOS “ARCO”

a. **A**cceso
b. **R**ectificación
c. **C**ancelación
d. **O**posición



Obligaciones del responsable del fichero

OBLIGACIÓN A INFORMAR SOBRE LA REALIZACIÓN DE VIDEOVIGILANCIA

1. Carteles

Obligaciones del responsable del fichero

2. Impresos informativos

a. Existencia del fichero o tratamiento de datos de carácter personal, motivo de la captación de las imágenes y destinatarios finales de la grabación o de la información resultante.

b. La identidad y datos de contacto del responsable del tratamiento, para que cualquier persona pueda dirigirse a este.

c. Además, el responsable del tratamiento debe proveer de impresos y procedimientos para ejercitar los derechos de acceso, rectificación, cancelación y oposición (**ARCO**) por cualquier individuo afectado. Si en ese momento no tiene impresos en papel, debe disponer de los medios necesarios para poder imprimirlos y proporcionarlos al interesado.

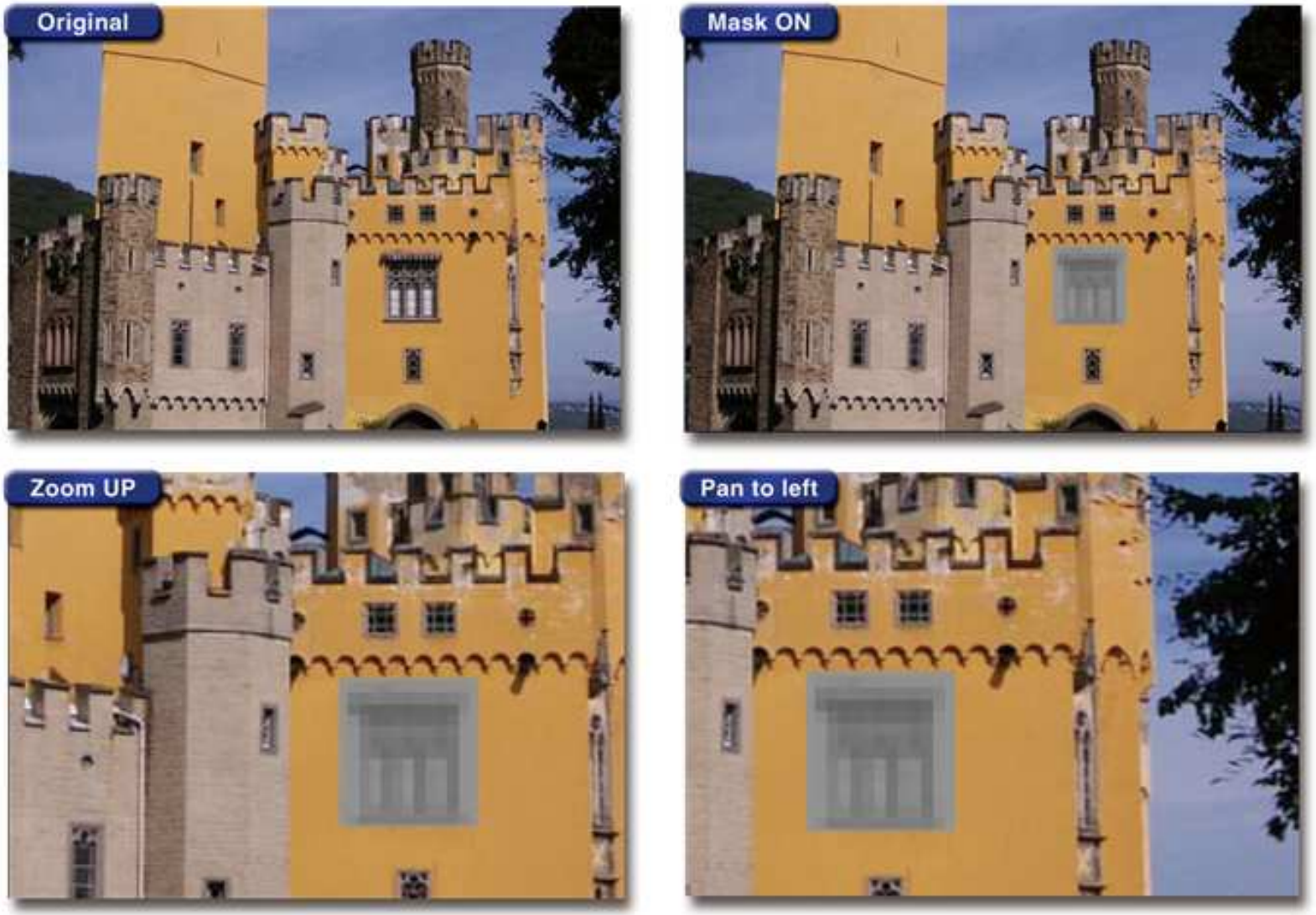
Contrato que regula el tratamiento de imágenes por terceros

Identificar la finalidad del tratamiento de los datos por el encargado.

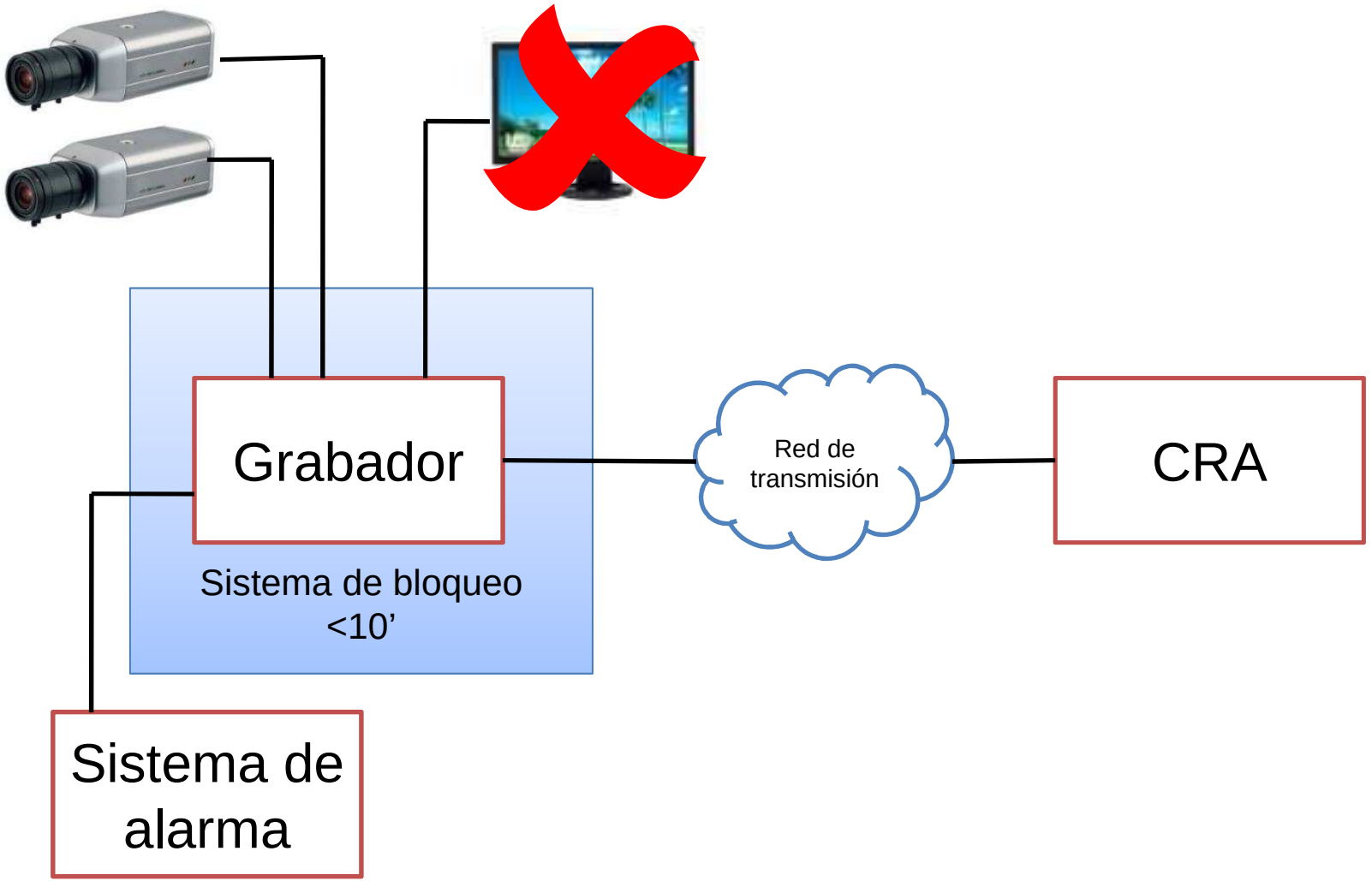
Establecer expresamente que los datos son tratados conforme a las instrucciones del responsable, y que no se aplican con otro fin distinto al que figure en el contrato.

Estipular las medidas de seguridad que el encargado está obligado a cumplir.

Máscara de privacidad



Configuración registro de imágenes



VIDEO-ANÁLISIS

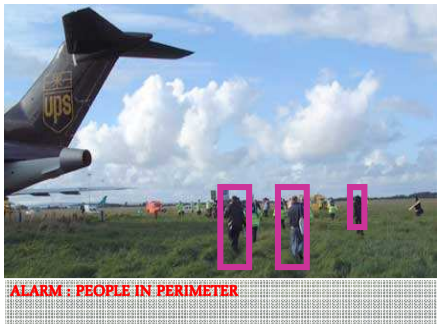
DAVANTIS

YOUR VIDEO ANALYSIS PARTNER

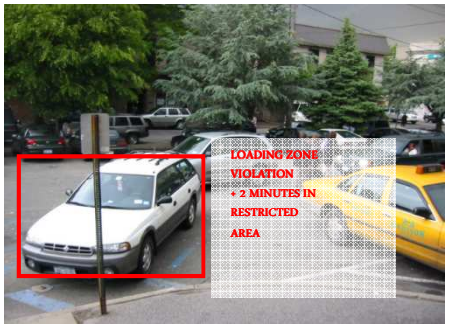
Qué hace?

- Mediante técnicas de Visión por computador, interpreta las imágenes y genera alarmas
- Puede detectar situaciones de riesgo
- Permite ver la detección y guardarla en vídeo
- Convierte una instalación de CCTV en un sistema activo

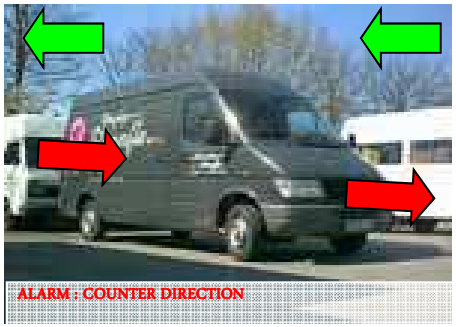
Daview



Detección de personas



Detección de vehículos



Dirección del movimiento

VIDEO-ANÁLISIS

ARQUITECTURA

Sistema Daview

+

Monitor + teclado + ratón
+ tarjeta de sonido

VIGILANTE

+

ADSL con IP fija

CENTRAL RECEPTORA

Casos de éxito

Entorno: Huerto Solar Conectividad: Router 3G

Recepción Alarma: CRA

Casos de éxito

Entorno: Huerto solar **Conectividad: ADSL (antenas)**

Recepción Alarma: CRA

Casos de éxito

Entorno: Cable cobre **Conectividad: Red local**

Recepción Alarma: Vigilante Seguridad

Casos de éxito

Casos de éxito

Gestión Puntos de Venta

Sistema POS

Análisis del punto de venta

Banking

The video surveillance in banking institution not only about protecting against thieves, but it is also providing more safer environment for staff members and customers. From a small town facilities to large offices with many branches, Samsung provides customized solution for each facility.

Main Mission

- Prevent theft
- Provide secure environment

Configuration (Network System)

Network Camera

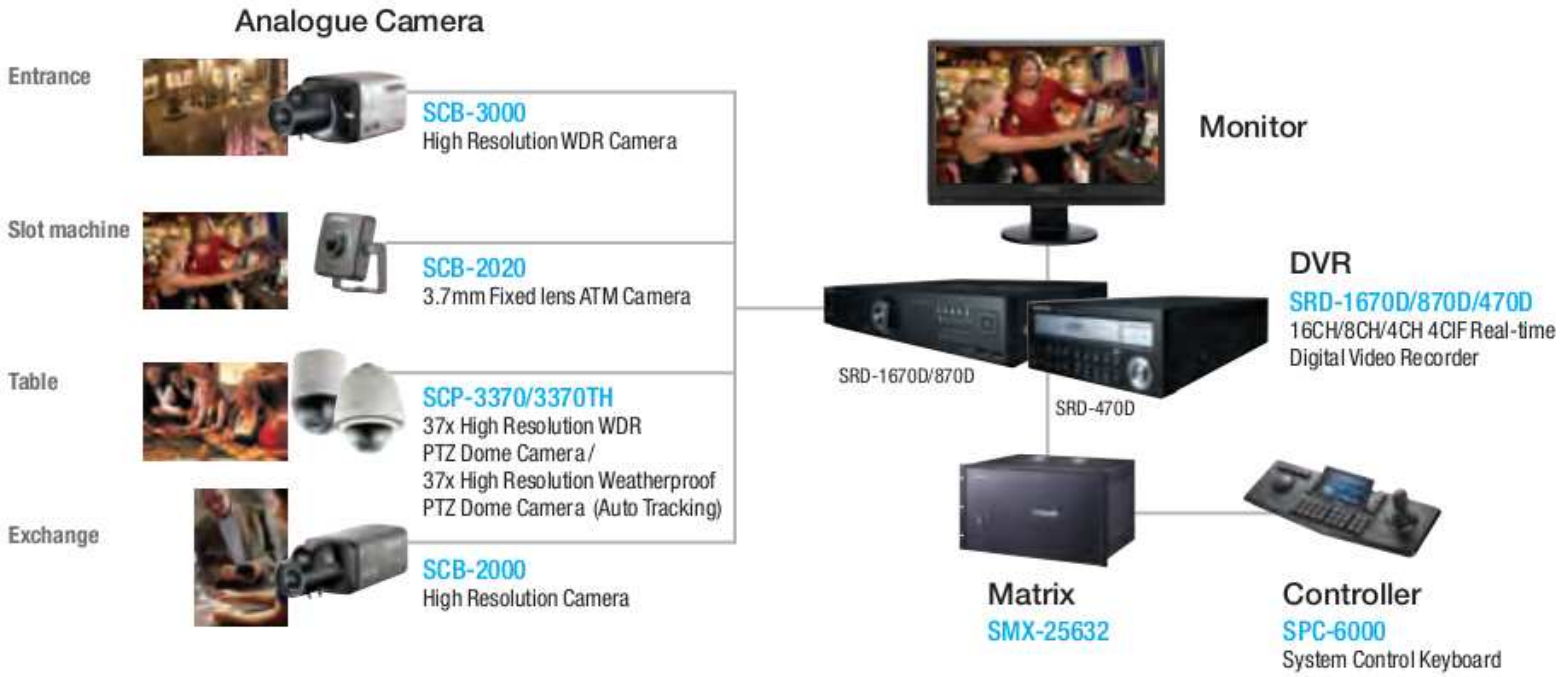
Casino

Gaming facilities such as casino and other entertainment operations need the most powerful tool for high surveillance. The clear capture of the sleight of hand and quick movement is what you need the most. Samsung's CCTV products can meet the needs and also guarantee to provide enjoyable and safe moment to customers who visit the facilities.

Main Mission

- Help customers managing
- Prevent cheating and deter criminal actions
- Provide safety environment to customers

Configuration (Analogue System)



City & Road Surveillance

Samsung's security solution offers useful tool for city surveillance in protecting citizens from theft and other crimes. It is also very helpful for road surveillance. Our solution helps to create a secure environment by informing watchers of any criminal situations.

Main Mission

- Protect citizens and property
- Increase urban safety and city value

Configuration (Network System)

Network Camera

SNP-3430H
4CIF 43x Weatherproof
Network PTZ Dome Camera

SNP-3370TH
4CIF 37x Weatherproof
Network PTZ Dome Camera

SNP-5200H
1.3M HD 20x Weatherproof
Network PTZ Dome Camera

SNZ-5200

+

SHB-4300H

+

SCU-VAC

SNZ-5200
1.3M HD 20x Network Zoom Camera +
SHB-4300H (Outdoor Housing)
+ SCU-VAC (Positioning System)

CMS

NET-i viewer

NVR

SRN-1670D
16CH Network Video Recorder

SCU-2370
37x High Resolution
Weatherproof
Positioning System

Encoder

SPE-100
1CH Network
Video Encoder

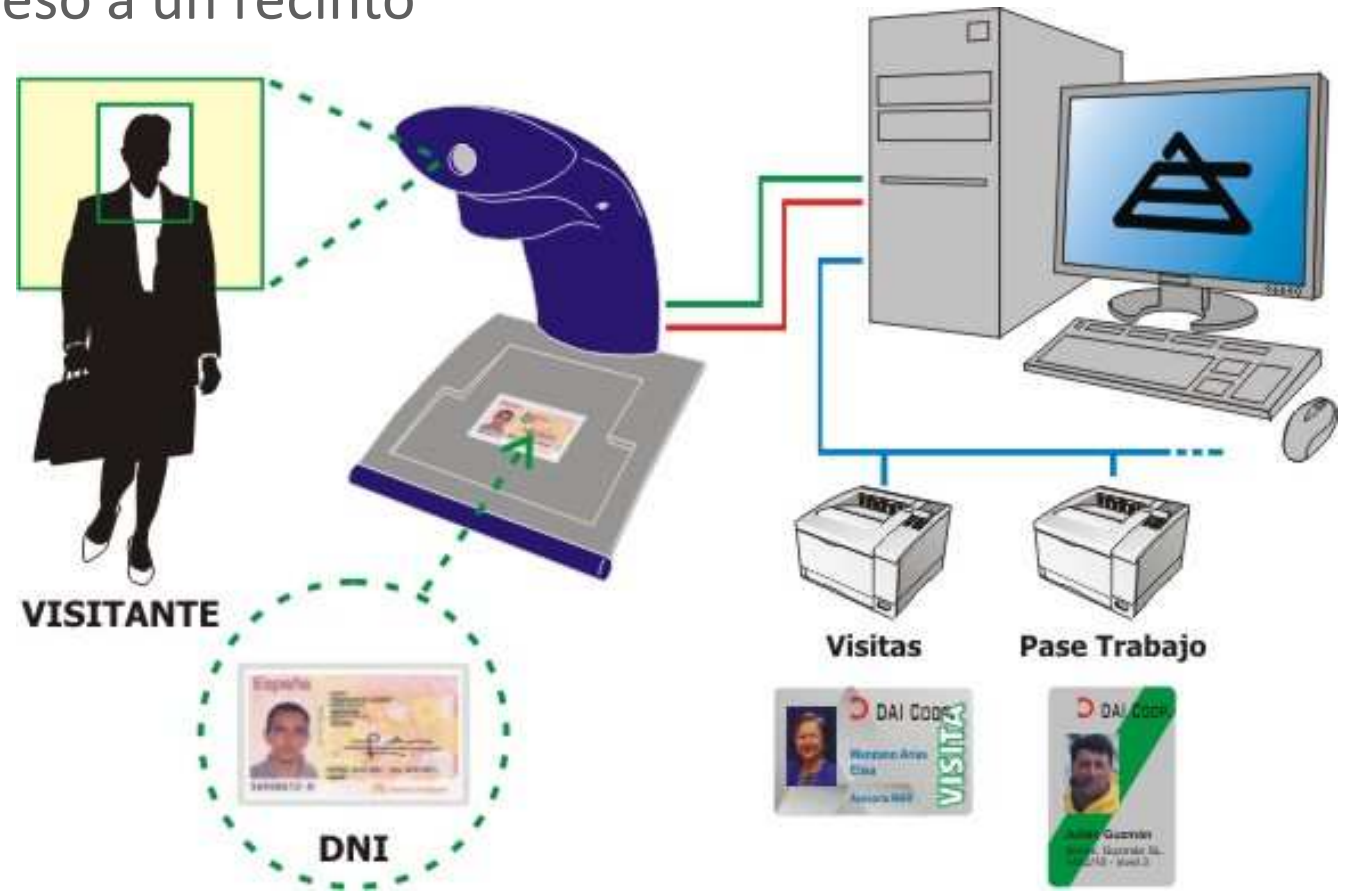
Control de Accesos

Concepto

Control de Accesos

Acreditaciones

Permite la creación y mantenimiento del soporte físico de acreditación personal, indispensable para la gestión de acceso a un recinto



Control de Accesos

Antipassback

impide que una acreditación de identificación pueda usarse en más de una ocasión para acceder a un recinto sin haber informado previamente de la salida

Control de aforos

1. Saber cuanto personal hay

2. Saber cuantos visitantes hay

Control de Accesos

Control de visitas

Permite obtener la información sobre las personas que hay en cada instante en la instalación, visitas registradas en un determinado período, visitas realizadas por una determinada persona, etc.

❖ Gestión de Entradas y Salidas de visitantes,

❖Generación de acreditaciones.

Sistemas contra Incendios

Teoría del fuego

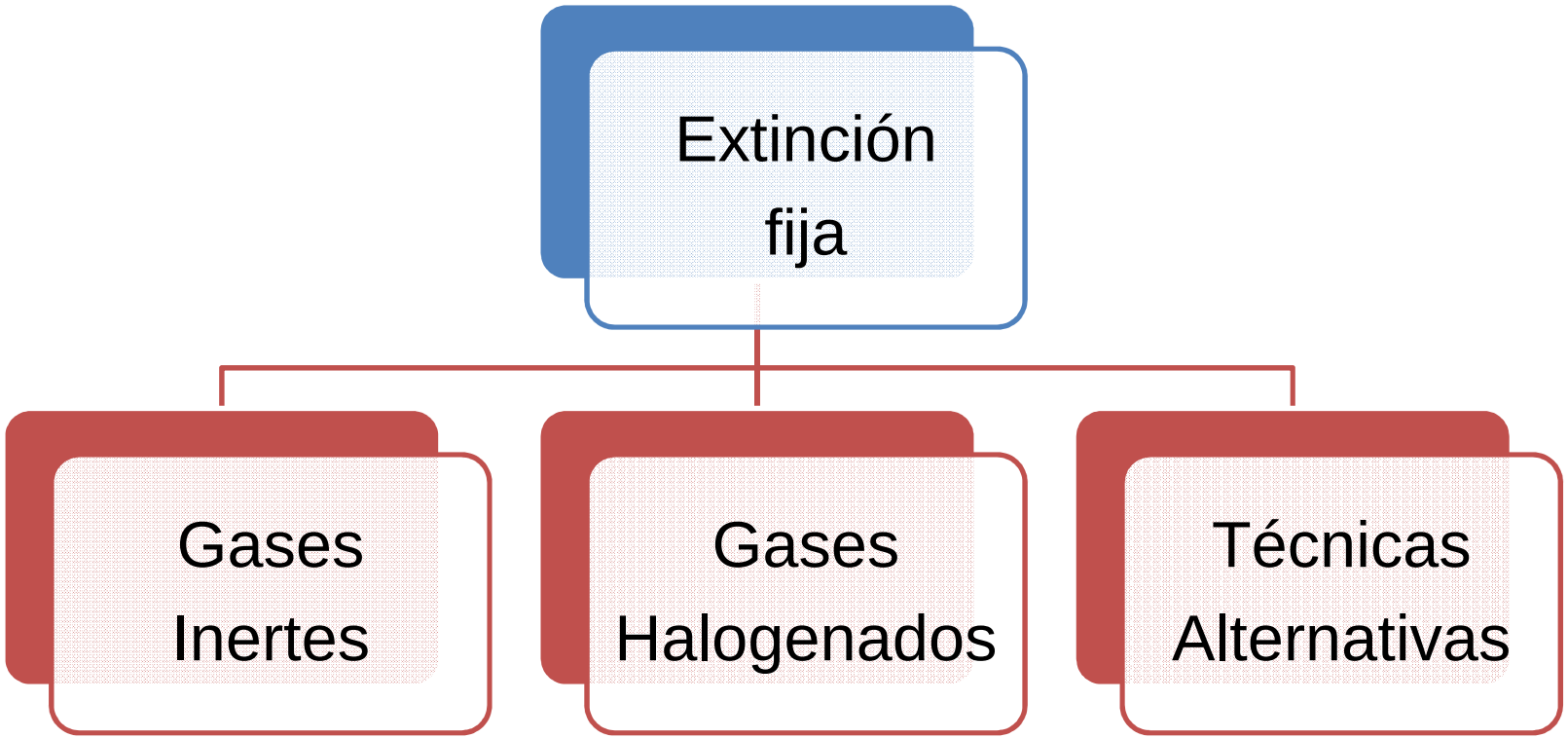
Los elementos necesario para que exista "fuego" deben ser siempre tres:

combustible, comburente y temperatura.

Para que progrese, la energía desprendida en el proceso tiene que ser suficiente para que se produzca la **reacción en cadena**

Si uno de estos cuatro elementos no se encuentra presente **no habrá fuego**

Extinción de incendios



Agua nebulizada

La extinción se produce por 3 acciones diferentes:

1. **Enfriamiento por absorción del calor, al vaporizarse el agua.**
2. **Atenuación de la transmisión de calor, por radiación.**
3. **Desplazamiento del oxígeno en el foco del fuego, por efecto de evaporación**

Integración de sistemas

Integración de sistemas

Control Integral de Seguridad

Visualización y control único

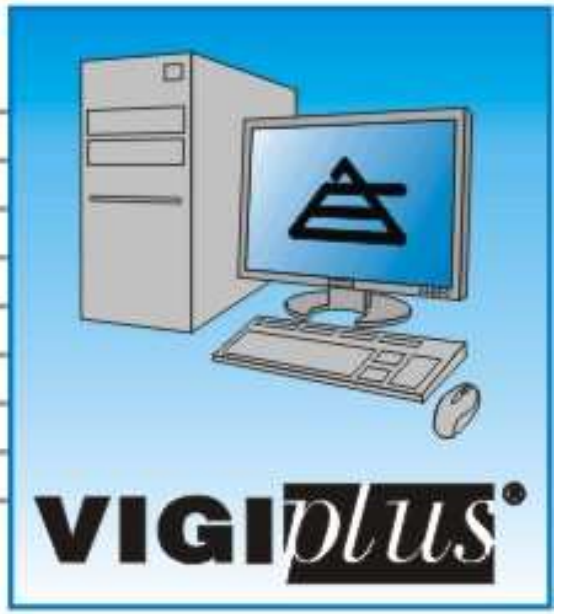
Herramienta indispensable para la toma rápida de decisiones operativas

Interacción entre sistemas

Gestión de históricos de incidencias

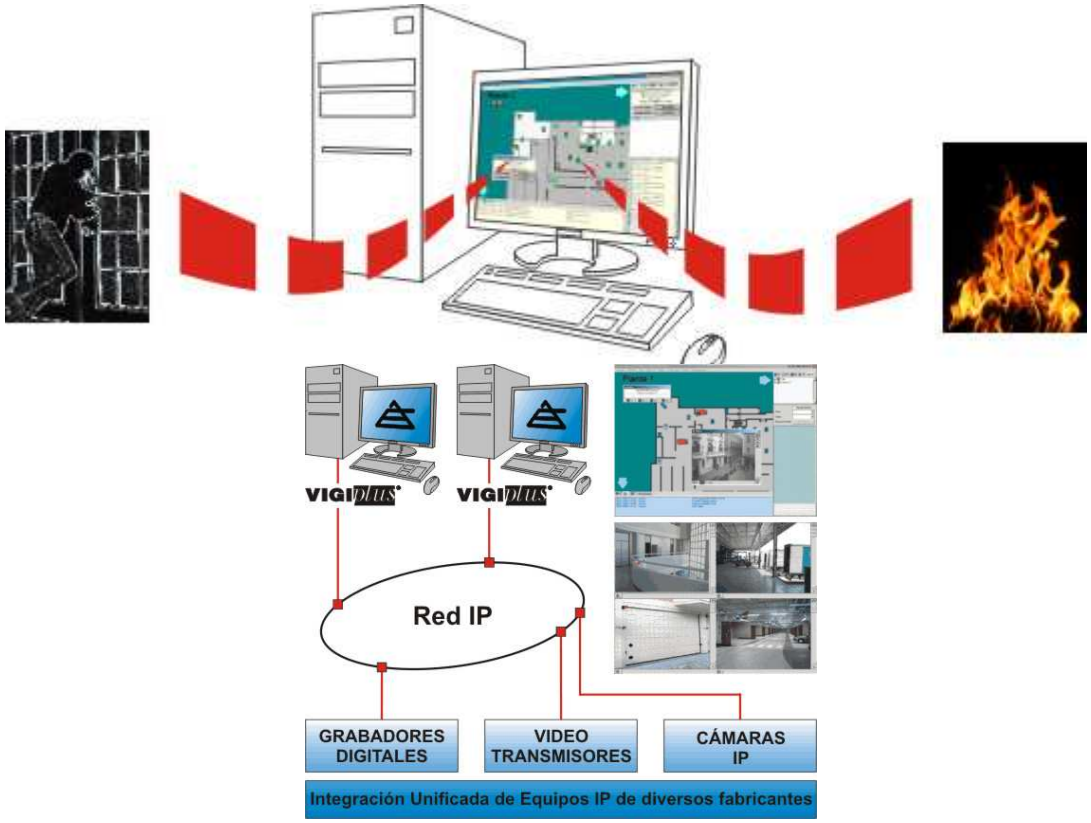
Integración de sistemas

- ✓ Incendio
- ✓ Intrusión
- ✓ Terminales de C. Accesos
- ✓ Lectores de Matrícula
- ✓ Vídeo Wall
- ✓ Vídeo Digital
- ✓ Vídeo Analógico
- ✓ Interfonía - Megafonía
- ✓ Automatización y Servicios Técnicos



Integración de sistemas

Gestión de alarmas de diferentes sistemas



Herramienta indispensable para la toma rápida de decisiones operativas

Bibliografía

www.casmar.es

www.ziton.com

www.hi-fog.com

www.sfedynameco.com

www.desico.com

www.davantis.com

www.acti.com

www.panasonic.com

www.samsung.com

www.utcfireandsecurity.com

www.interlogix.com

www.insht.es

Orden INT 314

Orden INT 316

Orden INT 317

Secretaria general técnica
Ministerio del interior

¿PREGUNTAS?